AMC PAMPHLET **AMCP 706-411**

ENGINEERING DESIGN HANDBOOK

VULNERABILITY OF COMMUNICATION-ELECTRONIC AND ELECTRO-OPTICAL SYSTEMS (EXCEPT GUIDED MISSILES) TO ELECTRONIC WARFARE

PART ONE
INTRODUCTION AND GENERAL APPROACH TO ELECTRONIC WARFARE VULNERABILITY (U)

NATIONAL SECURITY INFORMATION
Unauthorized Disclosure Subject to Criminal Sanctions

CLASSIFIED BY: CG USA ECOM
EXEMPT FROM GENERAL DECLASSIFICATION
Schedule of Executive Order 11652
EXEMPTION CATEGORY 3
DECLASSIFY ON 31 December 1989

HEADQUARTERS, US ARMY MATERIEL COMMAND **JANUARY 1976**

(U) LIST OF ILLUSTRATIONS

(U) LIST OF ILLUSTRATIONS

(U) LIST OF ILLUSTRATIONS (Con't.)

(U) LIST OF ILLUSTRATIONS (Con't.)

(U) LIST OF TABLES

(U) LIST OF TABLES

PREFACE

The Engineering Design Handbook Series of the US Army Materiel Command is a coordinated series of handbooks containing basic information and fundamental data. The handbooks are authoritative reference books of practical information and quantitative facts helpful in the design and development of materiel that will meet the tactical needs of the Armed Forces.

The objectives of this handbook series are: (1) to collect diverse sources of information unique to the determination of the vulnerability to electronic warfare of all types of communication-electronic and electro-optical equipment/systems, exclusive of guided missiles, in order to conserve time, materials, and money in the successful design of new equipment; (2) to provide guidance in capsule form for new personnel, Armed Forces contractors, or experienced design engineers in other fields who require information about vehicle electrical systems; (3) to supply current fundamental information; and (4) to place the reader in a position tion to use new information generated subsequent to the publication of this handbook. To meet these objectives, the handbook has been written to provide the necessary background regarding the vulnerability of military electromagnetic systems to electronic warfare (EW).

This handbook series includes chapters on basic concepts of vulnerability and computational methods for determining the EW vulnerability of tactical and satellite communications, surveillance and target acquisition radars, avionics, and electro-optical systems. The series consists of six separate handbooks, i.e.,

1. AMCP 706-411 Chapter 1 and 2
2. AMCP 706-412 Chapter 3
3. AMCP 706-413 Chapter 4
4. AMCP 706-414 Chapter 5
5. AMCP 706-415 Chapter 6
6. AMCP 706-416 Chapter 7.

The various handbooks are designed to be ordered and used separately; however, it is recommended that AMCP 706-411—which provides the introduction and general approach to EW vulnerability—be ordered to accompany the particular chapter(s) of interest. An index of the complete series is contained in each handbook. An abbreviated Table of Contents of the other handbooks of the series is contained in each of the separate handbooks.

This handbook was prepared by the Electronic Defense Laboratories of GTE Sylvania, Mountain View, CA, under subcontract to the Research Triangle Institute, Research Triangle Park, NC, prime contractor to the US Army Materiel Command. Mr. Robert Stone, GTE Sylvania, served

as Project Leader. Technical guidance and coordination were provided by a committee under the direction of Mr. Simon Cohen, Electronic Warfare Laboratories, US Army Electronics Command, Ft. Monmouth, NJ.

The Engineering Design Handbooks fall into two basic categories–those approved for release and sale, and those classified for security reasons. The US Army Materiel Command policy is to release these Engineering Design Handbooks in accordance with current DOD Directive 7230.7, dated 18 September 1973. All unclassified Handbooks can be obtained from the National Technical Information Service (NTIS). Procedures for acquiring these Handbooks follow:

a. All Department of Army activities having need for the Handbooks must submit their request on an official requisition form (DA Form 17, dated Jan 70) directly to:

Commander
Letterkenny Army Depot
ATTN: AMXLE-ATD
Chambersburg, PA 17201

(Requests for classified documents must be submitted, with appropriate "Need to Know" justification, to Letterkenny Army Depot.) DA activities will not requisition Handbooks for further free distribution.

b. All other requestors–DOD, Navy, Air Force, Marine Corps, nonmilitary Government agencies, contractors, private industry, individuals, universities, and others–must purchase these Handbooks from:

National Technical Information Service
Department of Commerce
Springfield, VA 22151

Classified documents may be released on a "Need to Know" basis verified by an official Department of Army representative and processed from Defense Documentation Center (DDC), ATTN: DDC-TSR, Cameron Station, Alexandria, VA 22314.

Comments and suggestions on this Handbook are welcome and should be addressed to:

Commander
US Army Materiel Development and
Readiness Command
Alexandria, VA 22333

(DA Forms 2028, Recommended Changes to Publications, which are available through normal publications supply channels, may be used for comments/suggestions.)

DEPARTMENT OF THE ARMY
HEADQUARTERS UNITED STATES ARMY MATERIEL COMMAND
5001 Eisenhower Ave, Alexandria, VA 22333

AMC PAMPHLET
No. 706–411

5 JANUARY 1976

ENGINEERING DESIGN HANDBOOK
VULNERABILITY OF COMMUNICATION-ELECTRONIC AND ELECTRO-OPTICAL SYSTEMS (Except Guided Missiles) TO ELECTRONIC WARFARE SERIES

PART ONE

INTRODUCTION AND GENERAL APPROACH TO ELECTRONIC WARFARE VULNERABILITY

TABLE OF CONTENTS

TABLE OF CONTENTS (Con't.)

(S) CHAPTER 2. GENERAL APPROACH TO VULNERABILITY OF COMMUNICATION-ELECTRONIC AND ELECTRO-OPTICAL SYSTEMS TO ELECTRONIC WARFARE

TABLE OF CONTENTS (Con't.)

TABLE OF CONTENTS (Con't.)

TABLE OF CONTENTS (Con't.)

Paragraph Page

(S) CHAPTER 5. ELECTRONIC WARFARE VULNERABILITY OF AVIONICS (U)

APPENDIX C. THEORETICAL SUSCEPTIBILITY OF NAVIGATION EQUIPMENT (AN/ARN-92 LORAN-D RECEIVER)

APPENDIX D. THEORETICAL SUSCEPTIBILITY OF A MULTIFUNCTION SYSTEM (HELMS)

TABLE OF CONTENTS (Con't.)

TABLE OF CONTENTS (Con't.)

TABLE OF CONTENTS (Con't.)

TABLE OF CONTENTS (Con't.)

Paragraph Page

APPENDIX K. OTHER COMMUNICATION SATELLITE SYSTEMS

DEPARTMENT OF THE ARMY
HEADQUARTERS UNITED STATES ARMY MATERIEL COMMAND
5001 Eisenhower Ave, Alexandria, VA 22333

AMCP PAMPHLET
NO. 706-412

6 January 1976

ENGINEERING DESIGN HANDBOOK
VULNERABILITY OF COMMUNICATION–ELECTRONIC AND ELECTRO-OPTICAL SYSTEMS (EXCEPT GUIDED MISSILES) TO ELECTRONIC WARFARE SERIES

PART TWO

ELECTRONIC WARFARE VULNERABILITY OF TACTICAL COMMUNICATIONS

TABLE OF CONTENTS

TABLE OF CONTENTS (Con't.)

TABLE OF CONTENTS (Con't.)

(C) CHAPTER 3. ELECTRONIC WARFARE VULNERABILITY OF TACTICAL COMMUNICATIONS (U)

TABLE OF CONTENTS (Con't.)

TABLE OF CONTENTS (Con't.)

TABLE OF CONTENTS (Con't.)

TABLE OF CONTENTS (Con't.)

TABLE OF CONTENTS (Con't)

TABLE OF CONTENTS (Con't.)

CHAPTER 1

INTRODUCTION (U)

1-1 (U) BACKGROUND OF THE VULNERABILITY HANDBOOK

1-1.1 (U) GENERAL

AR 105-87 defines Electronic Warfare (EW) as "military action involving the use of electromagnetic energy to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum". This handbook will present information that should guide equipment/system developers to develop equipments/systems with the capability "to retain friendly use of the electromagnetic spectrum" despite hostile EW actions. This is vital, because, with the Army's heavy dependence upon communication-electronic and electro-optical systems as well as electromagnetically aided weapons, the nullification of such systems by enemy EW action may spell the difference between victory or defeat in battle.

While the Army has been aware of this for a long time, events in the 1973 Israeli-Arab war lent greater urgency to this problem. To quote from an AMC letter of 2 January 1974, subject: "AMC Policy on Electronic Warfare":

> "Since World War II, the US Army has had a continuing program in Electronic Warfare (EW). In military operations, however, the Army's exposure to hostile EW or to hostile electromagnetically controlled weaponry has been minimal. Present and projected threat estimates indicate that this will not be the case in the future, and that the Army needs to improve its posture substantially both offensively and defensively in this program area."

For the Army to substantially improve its "defensive" EW posture, it must determine the vulnerability of its systems to hostile EW actions and determine what measures (technical and operational) can be taken to eliminate or minimize vulnerability. This handbook will be of value in accomplishing this objective.

The contribution that electronic warfare can make to success or failure on the battlefield is not immediately obvious, for, unlike bullets or artillery projectiles, the destruction wrought by the electronic bullets is not necessarily visible to the eye. Yet, for example, by "cutting-off" communications between a commander and his troops, EW can cause more damage than firepower alone. One must consider EW as another weapon in an enemy's arsenal of weapons and that an enemy will employ EW when it is to his advantage to do so. Just as any other weapon, the Army must be prepared to counter the enemy's EW weapon or pay a heavy price.

1-1.2 (U) PURPOSE

As part of its continuing program in electronic warfare, the Army has sponsored (and is sponsoring) many EW vulnerability studies. A great amount of the time, effort, and funds invested in the studies could be saved if EW vulnerability information were readily available for similar systems on which EW vulnerability studies have been conducted. Considerable amounts of EW vulnerability data have been generated; however, the information is scattered throughout innumerable classified documents. This handbook collects the scattered data—divorcing

them from specific end items of equipment—and consolidates the data into a single series of classified documents, together with a discussion and interpretation of the data. Thus, development personnel—concerned with the EW vulnerability of their systems—will be saved time and effort in attempting to locate and apply appropriate information or conducting EW vulnerability studies. To provide a continuing and up-to-date data base, some studies will still have to be conducted. Sample calculations are used throughout the text to illustrate the theory and ideas presented.

1-1.3 (U) SCOPE

This handbook covers investigations, studies, and analyses concerned with the vulnerability to electronic warfare (EW) of all types of communication-electronic (CE) and electro-optical (EO) equipment/systems, exclusive of guided missiles. It includes the various EW threats, present and future, which US communication-electronic and electro-optical systems may face in the field.

Elements comprising the handbook include:

(1) Factors that determine system vulnerability to EW—i.e., susceptibility, accessibility, interceptibility, feasibility, and tactics

(2) Steps, theoretical and experimental, that constitute a vulnerability investigation

(3) Effects of ECM modulations on different classes of equipment; e.g., fm radio, pulse Doppler radar, noncoherent moving target indicator (mti)

(4) Specific jamming-to-signal ratios J/S, and the effect of such J/S on the performance capabilities of the equipment exposed.

1-1.4 (U) HANDBOOK CONTENT

This handbook is presented in seven chapters. Chapters 1 and 2 introduce the basic concepts of vulnerability. Each of the remaining five chapters is designed as a complete treatise on its respective CE and EO subject matter. The overall content of each chapter is described in the paragraphs that follow.

1-1.4.1 (U) Introduction to the Vulnerability Handbook (Chapter 1)

Chapter 1 serves as an introduction to the handbook and presents the general subject of electronic warfare as it relates to vulnerability assessment. The chapter contains four major paragraphs:

(1) 1-1 Background of the Vulnerability Handbook

(2) 1-2 Electronic Warfare

(3) 1-3 Intelligence Coordination

(4) 1-4 Most Pertinent Publications on Electronic Warfare Guidance.

The paragraphs on electronic warfare provide a "layman's" introduction to the concept of EW, including identification of its component parts, the need for intelligence inputs, and the concepts of command and control of EW. Par. 1-5 provides a glossary of terms most frequently encountered in the field of EW.

1-1.4.2 (U) General Approach to Vulnerability of Communication-Electronic and Electro-Optical Systems to EW (Chapter 2)

Chapter 2 is a working explanation of vulnerability to EW. The subject matter is presented in four main paragraphs:

(1) 2-1 Introduction

(2) 2-2 Philosophy of Vulnerability to Electronic Warfare

(3) 2-3 EW Threat Precepts

(4) 2-4 Models of the EW Environment for Analysis Purposes.

The elements of vulnerability are identified and their relationship is shown. The Soviet threat capability is discussed, with emphasis on tactical employment, and the significance of threat modeling for vulnerability assessment is identified.

The different types of models of EW environment are outlined, with an explanation of the construction and utility of each type of model. Two Appendices are provided that list and define some of the existing models used in EW vulnerability analyses, and Soviet signal intercept systems.

1-1.4.3 (U) EW Vulnerability of Tactical Communications (Chapter 3)

Chapter 3 deals with the vulnerability of tactical communications and is presented in four major paragraphs:

(1) 3-1 Introduction

(2) 3-2 ECM Susceptibility Level

(3) 3-3 EW Threat Models

(4) 3-4 Vulnerability.

The susceptibility of both tactical and trunk systems is discussed in terms of ECM modulations and their effects on equipment performance. The level of jamming required is analyzed. Current threat data are summarized with direction on how to obtain updating through intelligence channels. Vulnerability is examined with respect to its elements, simulations, and critical parameters. A sample problem solution is given for the assessment of the vulnerability of a communication network.

1-1.4.4 (U) EW Vulnerability of Ground-Based and Airborne Surveillance and Target Acquisition Radars (Chapter 4)

Chapter 4 covers the vulnerability assessment technique for surveillance and target acquisition radars. The chapter is presented in five major paragraphs:

(1) 4-1 Introduction

(2) 4-2 Ground-Based and Personnel and Field Detection Radars

(3) 4-3 Airborne Vehicle Detection and Ground Mapping Radars

(4) 4-4 Weapon Location Radars

(5) 4-5 Meteorological Radars.

Each paragraph is complete within itself and identifies the radar system tactical role and employment concepts. Pertinent characteristics of the radar class are discussed, and the means of assessing the system vulnerability are identified.

1-1.4.5 (U) EW Vulnerability of Avionics (Chapter 5)

Chapter 5 discusses the assessment of the vulnerability of avionic systems. It is presented in four major paragraphs:

(1) 5-1 Introduction

(2) 5-2 EW Threat to Avionics

(3) 5-3 EW Vulnerability of Avionic Equipment

(4) 5-4 The Impact of EW Vulnerability on the Selection of Avionic Configurations.

The avionic systems are identified by class such as Communication, IFF, Terrain Avoidance Radar, and Navigation Systems. The general threat to these systems is discussed, and the system vulnerability criteria are identified. Steps to be taken in analysis are described, and methods for data reduction and presentation are explained. A discussion on mutual interference problems and mission profile as it affects vulnerability and the effects of EW vulnerability on air mobility missions completes the chapter.

1-1.4.6 (U) Optical/Electronic Warfare Vulnerability of Electro-Optic Systems (Chapter 6)

Chapter 6 covers the vulnerability assessment of electro-optical systems. It is divided into three major paragraphs:

(1) 6-1 Introduction

(2) 6-2 Vulnerability of Electro-Optic Systems

(3) 6-3 Optical/Electronic Counter-Measures.

This chapter describes the electro-optic equipments employed, their tactical employment and deployment requirements, the vulnerability aspects of the different classes of systems, the potential threats to these systems, and concepts for electro-optic counter-countermeasures. Specific approaches to determining the degree of susceptibility, interceptibility, and accessibility of the electro-optic systems are discussed.

1-1.4.7 (U) EW Vulnerability of Satellite Communications (Chapter 7)

EW vulnerability of satellite communications is addressed in four major paragraphs:

(1) 7-1 Introduction

(2) 7-2 Satellite Communication Systems

(3) 7-3 Satellite Communication System Vulnerability

(4) 7-4 Satellite Antijamming Techniques.

A brief history of satellite systems is presented, continuing with discussions on active/passive systems and orbit considerations. Satellite transponder subsystems and ground terminals for communication links are described for both uhf and shf systems. A presentation of vulnerability assessment techniques leads to a description of the susceptibility of several existing systems, and vulnerability assessment examples are provided for user assistance. Electronic counter-countermeasure (ECCM) approaches are treated briefly. Six appendixes are included detailing Satellites, Earth Terminals, Phase I, and Phase II, other Communication Satellite Systems, and Space Ground Link Subsystems.

1-2 (U) ELECTRONIC WARFARE

1-2.1 (U) DEFINITION

AR 105-87 provides the following definition of electronic warfare:

"Electronic warfare (EW) is military action involving the use of electromagnetic energy to determine, exploit, reduce or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum. There are three divisions within EW:

(1) Electronic warfare support measures (ESM)

(2) Electronic countermeasures (ECM)

(3) Electronic counter-countermeasures (ECCM)."

Fundamentals of EW, USAFA, includes the following defining characteristics of electronic warfare:

"Although not included in official US Army definitions, we should note that EW is really dependent on the radiation of electromagnetic radiation and not on 'electronics' *per se*. Hence, EW includes systems using all forms of electromagnetic energy (e.g., radio, radar, infrared (IR), optical systems, lasers, etc.)."

For the purposes of this handbook, EW has been broadened to mean electromagnetic warfare. Table 1-1 shows the electromagnetic divisions for EW.

1-2.2 (U) BRIEF HISTORY OF ELECTRONIC WARFARE

The use of electronic warfare is not new. It had its modest beginnings early in World War I when the Germans used deceptive messages to exploit Russian communication intelligence (comint) operations during 1914. Electronic warfare support measures (ESM) had its beginning during the Battle of Jutland in 1918, when the British tracked the German fleet radio transmissions, allowing intercept of the fleet with tactical advantage and subsequent victory by the British.

Recognition of the value of ESM led the Germans to the use of ECM. British radio stations along the Mediterranean were jammed to support the escape of the German fleet from the Black Sea.

World War II placed the development of EW on its exponential increase. The dramatic expansion in electronic technology and changes in tactical warfare doctrine during this period brought about the development of the CE complex and the EW equipments and concepts to exploit and counteract the use of electronic systems. Early in the war, the Germans deployed a navigation system to direct bombing raids on Britain. The British responded with deception signals to disorient the Luftwaffe. The game of oneupmanship began with two successive iterations of the German navigation systems countered successfully by the British.

Denial jamming came of age following the emplacement of radar-directed coastal guns by the Germans along the French coast. The British employed jammers to protect their coastal shipping lanes. The Germans also proved adept at deceptive jamming by initiating short-term jamming against British radars and gradually increasing the jamming period over several days' span, making the interference appear as atmospheric in origin. Finally, they established a jamming period of sufficient duration to cover the escape of three cruisers from the harbor at Brest through the English Channel to their home ports.

During the Libyan campaign of 1942, the

TABLE 1-1 (U). EW SPECTRUM (U)

Nomenclature	Wavelength
Radio	dc to 1,000 μm
Infrared	1,000 μm to 0.75 μm
Visible Light	0.75 μm to 0.38 μm
Ultraviolet	0.38 μm to 0.01 μm

British applied communication ECM from modified bombers, and were successful in disrupting the tactical communication networks of the Germans. The Germans countered this by using fighter planes to shoot down the bombers.

Deployment of the Axis early warning radars in defense of the continent resulted in the use of chaff by the United States during its raids on the German homeland. The initial employment was very effective and was accomplished by handcutting and hand-dispensing of tinfoil. Eventually the German radar operators learned to distinguish the false targets by target velocity and altitude-change discrimination. By the end of the war, nearly all US bombers carried both chaff and jammers to counter the German air defense radar systems.

These examples point out a truism that for every measure there exists a countermeasure and that the battle of ECM vs ECCM is a never-ending one.

EW laboratories created during WW II continued the development of ESM and ECM systems along with ECCM concepts at an accelerated pace. The maximum use of EW occurred during the Southeast Asia conflict, where the most sophisticated equipment in the operational inventory was employed by the United States against the Soviet-developed weapon systems. Most notable was the use of airborne ECM against the SAM and EW radar complexes and the introduction of laser-directed weapons.

The most recent use of EW has been seen in the Israeli conflicts. ESM and ECM have been used extensively in the Israeli tactical operations with great success, especially in communication ECM.

The development of EW equipments is advancing in the state of the art at an exceptional rate, and design of CE and EO systems from the vulnerability viewpoint is more important than ever.

1-2.3 (U) ELEMENTS OF ELECTRONIC WARFARE

The definition of EW presented in par. 1-2.2.1 identifies a complex subset of modern warfare consisting of many interdependent elements. As the concept of EW evolved, these elements have been discretely identified and defined. The resulting structure of present day EW is presented in Fig. 1-1. Just as EW is broadened to include the entire electromagnetic spectrum, the interdependent elements also include the optical and electro-optical portions of the spectrum.

1-2.3.1 (U) Electronic Warfare Support Measures (ESM)

ESM is defined as that division of EW involving actions taken to search for, intercept, locate, record, and analyze radiated electromagnetic energy for the purpose of exploiting such radiations in support of military operations.

When designing to reduce vulnerability to ESM, one must be aware that each time the system radiates in the field, it is opening itself to intercept by the opposing force. The task of the designer is to minimize the amount of radiation required to perform the mission assignment and control the modulation and antenna characteristics to reduce probability of intercept.

ESM and signal intelligence (sigint) have much in common but should not be confused in a mission statement. ESM is employed for tactical support to ECM, ECCM, physical counter-action, target acquisition and avoidance, warning, and tactical maneuvers in the field. The equipment employed for this covers a wide range of capability. Communication, noncommunication, and electro-optical systems are monitored, located, and analyzed to provide the inputs required for effective tactics. The three major functions of ESM are target intercept, target location, and target identification.

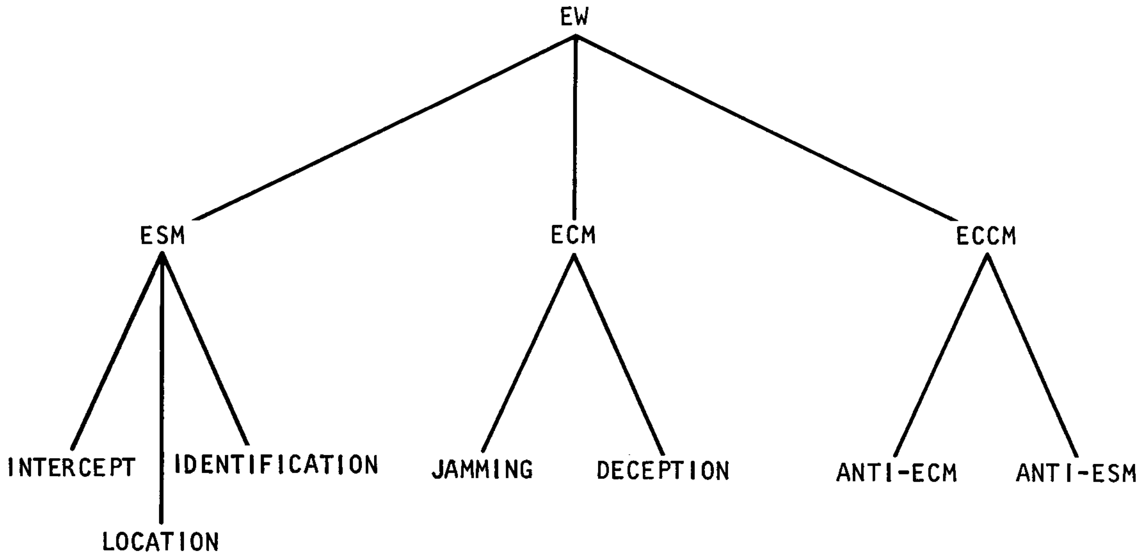


Figure 1-1. (U). Functional Organization of Electronic Warfare (U)

The major functions of sigint are communication and electronic intelligence collection for strategic use.

1-2.3.1.1 (U) Target Intercept

Intercept of enemy forces by their radiations provides warning data for all elements of the friendly tactical forces. Force size, makeup, and direction sometimes can be estimated and targets of opportunity established quickly through the effective use of ESM.

1-2.3.1.2 (U) Target Identification

Electronic order of battle can be obtained to complement tactical reconnaissance operations, and specific threat parameters are provided for support of ECM and ECCM operations. Tactical employment of integrated ESM also will provide sigsec improvements through the monitoring of friendly radiations.

1-2.3.1.3 (U) Target Location

Location of the emitters of an enemy force through direction finding operations provides the field commanders with data to support direct counteraction or avoidance tactics.

1-2.3.2 (C) Electronic Countermeasures (ECM)

(U) Electronic countermeasures (ECM) are actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. For the purposes of this handbook, electronic countermeasures include electronic and/or optical jamming and electronic and/or optical deception.

(C) ECM systems and techniques all have one thing in common: they deliver energy into an enemy receiver system. (Absorptive ECM operates by diminishing the amount of energy that normally would be returned to the enemy receiver system.) To accomplish this mission, ECM systems may be employed as airborne, ground-/sea-based, or spaceborne equipments. Expendable ECM normally is designed for one-time and unattended operation, to be placed in the vicinity of the enemy system receiving antenna through clandestine or air-dropped operations. ECM systems usually employ their own sensors for

threat qualification and radiation control, but may be pure emitters requiring ESM support for line-of-bearing data and frequency assignment. ECM encompasses a wide variety of modulation classes with multiple modulation capability available in most modern systems. Computer control of transmitters based upon received parameter data is well within the state of the art, and many of these systems are in development or are already fielded within the United States. There are indications that the Soviets also use computers to control their ECM systems.

(U) The ECM operations within a tactical force must interface with the ESM and sigint operations to prevent self-jamming of friendly forces or unintentional interference with intelligence collection efforts.

1-2.3.2.1 (U) Jamming

Jamming is the deliberate radiation, reradiation, or reflection of electromagnetic energy, with the object of impairing or denying the use of electronic or electro-optic devices, equipment, or systems by the enemy.

1-2.3.2.2 (U) Deception

Deception is the deliberate radiation, reradiation, alteration, absorption, or reflection of electromagnetic energy in a manner intended to mislead an enemy in the interpretation or use of information received by his electronic or electro-optic systems. There are two categories of deception:

(1) Manipulative–introducing alteration or simulation of friendly radiations to accomplish a false impression.

(2) Imitative–introducing radiations into enemy channels which imitate his own emissions, but with false information.

1-2.3.3 (U) Electronic Counter-Countermeasures (ECCM)

Electronic counter-countermeasures are that major subdivision of EW involving actions taken to ensure our own effective use of electromagnetic radiations in spite of the enemy's use of countermeasures. ECCM circuitry and options are determined following a vulnerability analysis conducted during the development cycle of the CE system. ECCM breaks down into two major categories: Anti-ECM and anti-ESM.

1-2.3.3.1 (U) Anti-ECM

The effectiveness of any ECM technique can be reduced or eliminated by proper design and inclusion of ECCM circuitry in a CE or EO system. Establishing the type of circuitry to be included is strongly dependent upon data on the EW threat the system must counter. If these data are available, they can be obtained through intelligence channels; if not available, estimates must be made of the threat capability. Multiple modulation capability, coupled with broad instantaneous bandwidths and sophisticated signal processing within an ECM system, makes ECCM design a difficult task, and complete invulnerability probably never can be achieved in view of the advancing technology. This does not diminish the necessity for a thorough evaluation of ECCM considerations. The same situation exists in the area of electro-optics.

When designing to reduce vulnerability to ECM, trade-offs must be made in system complexity and cost that are directed toward reducing the effect of energy that the opposing force can place within the information bandwidth of the victim system. All CE and EO systems are vulnerable to a certain degree, but good design can place an unrealistic burden upon the ECM systems to be faced. This is the area of ECCM design in which not only the technical characteristics but also the operational requirements and employment concepts of the system under design must be considered.

1-2.3.3.2 (U) Anti-ESM

Employment, deployment, and operational procedures have a major impact on the effec-

tiveness of EW against a CE or EO system. Since it is necessary first to intercept a victim before counteraction can take place, care in siting and using the system can become as effective a CCM technique as inclusion of circuitry. Procedures employed in sigsec are considered a form of ECCM when applied for that purpose. Once under ECM engagement, operating procedures can be applied which will improve the victim's capability to work through the ECM. Narrow banding, detuning, frequency shift, short-burst operations, and use of ECCM circuit options are examples of some of the procedural approaches which can be taken.

1-2.3.4 (U) Signal Intelligence (Sigint)

Sigint is a generic term that includes both communication intelligence and electronic intelligence. Communication intelligence (comint) consists of technical and intelligence information derived from foreign communications by other than the intended recipients. Electronic intelligence (elint) is the intelligence information product of activities engaged in the collection and processing–for subsequent intelligence purposes–of foreign noncommunication, and electromagnetic radiations emanating from other than nuclear detonations and radioactive sources.

Further subsets of elint are radar intelligence (radint), radiation intelligence (rint), and optical intelligence (opint). Radint refers to the technical data that are obtained through monitoring and analysis of radar emissions. Rint refers to the data that are obtained through monitoring and analysis of nonintentional emissions that emanate from sources such as motor generator sets and trucks that provide support to the CE or EO system. Opint refers to the data that are obtained through monitoring and analysis of electromagnetic emissions in the optical wavelengths.

Sigint and ESM activities are conducted within the same electromagnetic environment, but the end item of their operations is significantly different. ESM is employed for direct support of tactical operations, while sigint provides intelligence inputs to higher levels, such as the national level, or to field army command. For example, an ESM system might intercept, identify, and locate a counterbattery radar in support of a fire mission, while the sigint operation would monitor the radar characteristics to obtain any changes in parameters which may be of use in the design of EW equipment. Basically, ESM is intended for "immediate" tactical use, while sigint is intended for strategic purposes. However, there are occasions when either can serve the purpose of the other.

1-2.3.5 (U) Signal Security (Sigsec)

Sigsec is a generic term that includes both communication security (comsec) and electronic security (elsec). Comsec is the protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretations of the results of such study. Comsec includes cryptosecurity, physical security, and transmission security.

Elsec is the protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from their interception and study of friendly noncommunication electromagnetic radiations.

1-2.4 (C) APPLICATION OF ELECTRONIC WARFARE

1-2.4.1 (U) Employment

EW will be applied against a CE or CO system only after deliberate consideration of the effects it will achieve, and the operation will be a coordinated one. There are three basic capabilities to be considered for obtaining effective countermeasures: interceptibility, accessibility, and susceptibility. A fourth

capability consideration is the feasibility of fielding effective EW equipment. The interaction of these four elements plus tactics denotes the vulnerability of the CE or EO system under consideration. Given the feasibility of being faced with effective EW, the designer of CE and EO equipment must consider the application of the first three capabilities.

Interceptibility is the measure of the probability of detecting and recognizing a signal of interest. The enemy uses the intercepted victim signal data to set the jammer or receiver parameters for maximum effectiveness either in ECM or ESM. The problem faced by the interceptor is increased by time constraints and influenced by victim transmitter power, antenna or lens characteristics, bandwidth, propagation losses, operating techniques, and modulation characteristics. The CE or EO system designer can consider techniques to reduce interceptibility by predicting what the enemy must face in being able to detect and operate on the CE or EO system radiation.

Accessibility refers to the degree to which a victim system is open to influence or access by an interfering signal. Generally, there is a geometry situation that the victim can use to his advantage and antenna patterns and nonrepetitive transmissions can be used in denying access. In cases where the ECM receiver or sensor is not collocated with the jammer, antenna pattern, frequency shift, and variable scan rates can be most effective. These factors, among others, can be used by the system designer in reducing accessibility to his equipment.

Susceptibility is defined as the effect of an undesired signal upon the performance of a CE or EO equipment/system. This is strictly a function of the equipment design and is measured under laboratory or laboratory-like conditions. Therefore, the susceptibility of a CE or EO system is a critical function of its design. Sensitivity, stability, detection type, processing gain, bandwidths, automatic gain control (agc) parameters, and output devices all contribute to the susceptibility (good or bad) of the system.

1-2.4.2 (C) Deployment

(U) Interceptibility and accessibility of a target are strongly dependent upon the deployment concepts that surround it. The same is true for the EW system that can be directed toward the target. Tactical geometries restrict siting of both the EW and CE or EO victim equipment, and affect the tactical or operational vulnerabilities of the equipment under consideration. For instance, a countermortar/counterbattery (cmcb) radar normally is sited in defilade with a wide-sector scan mission. This usually denies direct access to the main beam from a ground-based jammer, and the accessibility is considered quite low for jamming. This is true for a ground-based ECM system with no encroachment over the forward edge of the battle area (feba), but two features make the radar accessible to ECM: it is close to the feba since its target is artillery or mortars, and it operates from a semi-fixed surveyed position.

(C) The short-range deployment makes the radar accessible from airborne platforms such as aircraft or air-delivered expendables, which can exploit the main beam and major sidelobes of the radar. The fixed position makes the radar accessible from ground-based expendables, which can be artillery- or drone-delivered around the radar and operate at very short range into its sidelobes and backlobes.

(C) Combat surveillance/target acquisition (csta) radars may be vulnerable to denial, deception, and confusion jamming through their main beam because of the clear line-of-sight emplacement. Range denial through noise jamming can hide the exact location of a target even though its bearing may be made obvious by a jamming strobe. False-target

generators also can be used to synthesize a large force where one does not exist.

(U) The preceding facts must be considered in vulnerability analysis and ECCM design, and CE systems must be provided with sufficient flexibility to make EW response difficult.

1-2.4.3 (C) Adaptability

The system designer can make a tremendous impact on enemy EW effectiveness by incorporating a wide variety of ECCM features in his system design and providing the operators with the capability of selecting the ECCM features they desire. The selection of ECCM circuitry and options must be a logical one, following a detailed vulnerability analysis early in the CE or EO system development cycle. In general, one ECCM fix will not be sufficient to assure good system performance in the presence of ECM because of the flexibility of jamming modulations. For example, wideband limiting followed by narrowband filtering (Dicke Fix) is suitable for reducing the effect of a swept cw jammer, but will not provide any benefit against a hunt-lockon ECM system. In fact, it could further degrade the system in the presence of jamming. Fixed-frequency diversity operation may be defeated by a dual-rf-modulation ECM system, but a frequency-hopping system might be very effective in forcing the jammer to barrage noise. Noise-riding threshold agc systems are effective against cw jamming, but pulse jamming could overcome the advantage. Shift to jittered prf could defeat the pulse jamming mode. It is clear that no one ECCM approach is best and the designer must build adaptability into his systems. This must be approached on the basis of cost-effectiveness and operational constraints. Good threat modeling will provide the data required to select the ECCM features most desirable and limit the complexity and cost of the CE system design.

1-3 (U) INTELLIGENCE COORDINATION

Design for reduction of vulnerability must take into account the capability of the hostile EW that the CE or EO system will have to contend with. A realistic threat model that is firmly based on approved DA or DOD intelligence inputs is required. However, there may be instances when hard intelligence is not available, particularly for some time in the future. Therefore, it may be necessary to postulate the EW threat based on best engineering judgment. This must be done in conjunction with the intelligence community.

EW threat models are available through specific intelligence channels within DA and the Army Materiel Command (AMC). In fact, there is direct intelligence support available within each agency and facility of AMC. This support is located in the Foreign Intelligence Office (FIO) of each facility. The FIO has a direct chain of access to the data, which are collected and generated under the cognizance of the Assistance Chief of Staff for Intelligence (ACSI) by the Foreign Science and Technology Center (FSTC) and the Missile Intelligence Agency (MIA). Once a project has been assigned to a given activity, all available intelligence data concerning that project can be obtained by working through the local FIO.

The objectives of the FIO are:

(1) Process user requirements for intelligence support.

(2) Acquire and/or collect information and/or materiel for user.

(3) Analyze and/or test information and/or materiel.

(4) Evaluate data and product studies and/or reports.

(5) Disseminate intelligence to satisfy user requirements.

(6) Assist users in application and interpretation of data.

(7) Consider potential threats and applicable state of the art at all appropriate decision points and continuously through the RDTE cycle.

1-4 (U) MOST PERTINENT PUBLICATIONS ON ELECTRONIC WARFARE GUIDANCE

The impact of electronic warfare on military operations has resulted in the generation of many doctrinal and operational guidelines for the field commanders. In addition, handbooks such as this one are being prepared to assist the CE and EO system designers in their tasks. This paragraph of the Vulnerability Handbook lists those regulations and directives that have the most applicability in supporting the design of a system for minimizing vulnerability to EW.

1-4.1 (U) COMMUNICATIONS-ELECTRONICS ELECTRONIC WARFARE (AR 105-87)

"This regulation establishes an electronic warfare (EW) policy that provides for the effective use of EW and its integration into military operations. The increased application of electronics in the development of weapon system control and guidance systems, command and control communications, and reconnaissance and surveillance systems has created new requirements for EW."

1-4.2 (U) ELECTRONIC COUNTER-COUNTERMEASURES (ECCM) (AR 105-2)

"This regulation promulgates policy, provides guidance, prescribes procedures, and defines responsibilities for achieving US Army objectives in the field of electronic counter-countermeasures (ECCM) and for promoting effective operations in a hostile electronic warfare environment."

1-4.3 (U) ELECTROMAGNETIC COVER AND DECEPTION (EC&D) (AR 105-5)

"This regulation promulgates policy, provides guidance, prescribes procedures, and defines responsibilities for electromagnetic cover and deception."

1-4.4 (U) ELECTRONIC WARFARE (FM 32-20)

"This manual provides doctrine and other necessary information for personnel engaged in planning and conducting electronic warfare (EW) and is a basic reference for commanders whose operations may be supported by EW. The manual discusses EW policies and responsibilities, outlines concepts for the conduct of EW, and provides examples of its uses."

1-4.5 (U) ELECTRONIC COUNTERMEASURES HANDBOOK (FM 32-20-1)

This draft handbook is a supplement to FM 32-20, providing an insight into the operational and technical factors surrounding the application of ECM in tactical situations. The subject matter incorporates planning, execution, and evaluation of ECM operations.

1-4.6 (U) FOREIGN INTELLIGENCE OFFICE HANDBOOK

"Each element of AMC required to have a FIO is expected to use this FIO Handbook as an aid to providing itself the best possible intelligence support in order that the policy of taking full advantage of our knowledge of foreign scientific, technological, and materiel developments may be implemented effectively."

1-5 (U) GLOSSARY OF TERMS ASSOCIATED WITH VULNERABILITY ASSESSMENT (U)

A

accessibility – The degree of being open to influence or access by an interfering signal, taking into consideration antenna patterns, propagation path, deployment, geometry, and timing. It is concerned with the problem of coupling interfering energy of appropriate frequency and modulation into the antenna of the intended victim.

angle deception repeater – A type of repeater jammer that repeats the victim's radar pulse with a 180-deg phase shift, resulting in increasing angle error determination by the victim radar.

angle noise – Tracking error introduced into radar by variations in the apparent angle of arrival of the echo from a target due to finite target size. This effect is caused by variations in the phase front of the radiation from a multiple-point target as the target changes its aspect with respect to the observer.

angular scintillation – A random fluctuation in the angle of echo arrival at a radar antenna caused by the apparent center of radiation of the echo wandering at random over the target limits.

antenna adaptation – This ECCM technique places an antenna null or nulls in the direction of the jamming source(s), thereby reducing the jammer amplitude to a minimum. The steering is typically electronic and is achieved by adjusting the relative phases and amplitudes of the incoming signal.

antijamming – The act of minimizing the effect of enemy electronic countermeasures (another term for ECCM).

authentication – A security measure designed to protect a communication system against fraudulent transmissions.

automatic scanning receivers – Receivers that can sweep automatically and continuously across a preselected frequency either to stop when a signal is found or to plot signal occupancy.

automatic search jammer – An intercept receiver and jamming transmitter system that automatically searches for and jams signals that have specific radiation characteristics. Also called a hunt-lockon jammer.

B

babbled voice jamming – A modulating signal composed of mixed voices engaged in simultaneous conversations.

backlobe jamming – Jamming through the backlobe of the victim receiving antenna.

bagpipes – A type of electronic jamming signal consisting of tones repeated continuously.

balloon reflectors – Balloon-supported reflectors to produce fraudulent echoes.

barrage jamming – Simultaneous electronic jamming over a broad band of frequencies.

barrage noise jammer – A jammer that radiates noise or noiselike power spread uniformly over a specified wide frequency band (wider than the bandwidth of the victim receiver).

birdnesting – Clumping together of chaff dipoles after they have been dispensed from an aircraft.

blossoming – The expansion of the echo on a radar scope display caused by the dispersal of the chaff elements.

break lock – The effect brought about by active ECM against a tracking radar that causes the radar to lose contact with its target.

burnthrough range – The maximum distance at which a specific radar can discern targets through the external interference being received, assuming that at a distance greater than the burnthrough range, the radar cannot detect targets.

C

chaff – Radar confusion reflectors—which consist of thin, narrow metallic strips of

various lengths and frequency responses—used to reflect echoes for confusion purposes. To be most effective, the strips are cut to a half-wavelength of the desired radar frequency.

chaff corridor – The result of aircraft dropping a continuous amount of chaff.

coincidence detection – An ECCM technique accomplished by comparing video from two successive interpulse intervals and detecting only those video signals having the same relationship in the two intervals.

communication intelligence (comint) – Technical and intelligence information derived from foreign communications by other than the intended recipients.

communication jamming (comjam) – Electronic jamming against any medium, using electromagnetic radiation to convey a message from one person, or headquarter (including machine) to another.

communication security (comsec) – The protection resulting from all measures designed to deny to unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretations of the results of such study. Communication security includes cryptosecurity, physical security, and transmission security.

constant false alarm rate (CFAR) – Signal detection techniques that maintain a constant probability of false alarm when exposed to undesired signals such as ECM, but also exhibit an acceptable detection probability for the desired radar echo signals.

counter-countermeasures (CCM) – Employment of techniques and tactics designed to decrease the effects of countermeasure activities against electronic and electro-optic equipment.

countermeasures (CM) – That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of agressor activity.

cross-eye – A track-breaking deception jammer that from two separate points detects signals, crosses the received signals to the opposite points, and retransmits the signals with 180-deg phase shifts.

D

decoy – A fraudulent electromagnetic or physical (e.g., corner reflector) target used to simulate a genuine target.

degradation – Reduction in serviceability. In electronic warfare, a reduction in the effectiveness of communication and other electromagnetic systems through countermeasures.

Dicke Fix – A technique designed to protect a receiver from fast sweep jamming, using a wideband if, a hard limiter, and a narrowband if.

diversity ECCM techniques – Diversity can be used to improve channel ECCM effectiveness. Space diversity, frequency diversity, and time diversity commonly are used. In space diversity, two independent systems are used (not physically collocated). In frequency diversity, different frequencies are used to carry the information simultaneously. In time diversity the message is sent at two different times. Naturally, combinations of these techniques can be implemented.

E

electromagnetic camouflage (elcam) – The use of electromagnetic shielding, absorption, and/or enhancement techniques to minimize the possibility of detection and identification of troops, materiel, equipment, or installations by hostile sensors employing radiated electromagnetic energy.

electromagnetic compatibility (emc) – The ability of communication and electronic equipments, subsystems, and systems, together with electromechanical and electro-optical devices, to operate in their intended operational environments without suffering or causing unacceptable degradation because of unwanted electromagnetic radiation or response. Radio-frequency interference reduction is an older term for electromagnetic compatibility and is considered to be synonymous with the newer term, electromagnetic compatibility, which is preferred.

electromagnetic pulse (emp) – An effect of nuclear explosions that may degrade radar, radio, and other electromagnetic systems through the induction of damaging transient voltages and currents.

electromagnetic signature – The electromagnetic radiation characteristics that are peculiar to a specific electronics-dependent system and thus provide a basis for identification of the system among many systems. The totality of electromagnetic signatures radiated by the systems of a given operational unit is called the electromagnetic profile of the unit.

electronic counter-countermeasures (ECCM) – That major subdivision of electronic warfare involving actions taken to ensure our own effective use of electromagnetic radiations despite the enemy's use of countermeasures.

electronic countermeasures (ECM) – That major subdivision of electronic warfare involving actions taken to prevent or reduce the effectiveness of enemy equipment and tactics employing or affected by electromagnetic radiation and to exploit the enemy's use of such radiations.

electronic deception – The deliberate radiation, reradiation, alteration, absorption, or reflection of electromagnetic radiations in a manner intended to mislead an enemy in the interpretation of data received by his electronic equipment or to present false indications to electronic systems.

electronic intelligence (elint) – The intelligence information product of activities engaged in the collection and processing, for subsequent intelligence purposes, of foreign, noncommunication, and electromagnetic radiations emanating from other than nuclear detonations and radioactive sources.

electronic security (elsec) – The protection resulting from all measures designed to deny to unauthorized persons information of value that might be derived from their interception and study of friendly noncommunication electromagnetic radiations.

electronic warfare (EW) – That division of the military use of electronics involving actions taken to prevent or reduce an enemy's effective use of radiated electromagnetic energy and actions taken to ensure our own effective use of radiated electromagnetic energy.

electronic warfare support measures (ESM) – That division of EW involving actions taken to search for, intercept, locate, and identify immediately radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, ESM provides a source of EW information required to conduct ECM, ECCM, threat detection, warning, avoidance, target acquisition, and homing.

electro-optical countermeasures (EOCM) – The use of electromagnetic radiation that degrades the victim electro-optical system.

electro-optics (EO) – Term used to describe the technology achieved through the union of optics and electronics. As presently applied, the term includes lasers, photometry (light intensity measurement), infrared, and various other types of visible and infrared

imaging systems; i.e., low-light-level television, optical contrast sensors, and signal processing devices.

electro-optic support measures (EOSM) – Action taken to detect and/or intercept victim electro-optic equipment. The characteristic electromagnetic signatures may be used to provide threat information.

emission control (emcon) – The management of electromagnetic radiations to counter an enemy's capability of detecting, or locating friendly emitters for exploitation by hostile action.

emission control orders – Orders referred to as emcon orders, used to authorize, control, or prohibit the use of electronic emission equipment.

enemy electronic order of battle – The identification, structure, and disposition of communication and other electronic systems of an enemy force.

expendable jammer – An electronic jamming transmitter, normally designed for one-time and unattended operation, to be placed in the vicinity of the enemy radio or radar receiving antenna through clandestine or air-dropped operations.

F

false target – An electromagnetic return, generated by a deception device, that results in the display of a nonexistent target(s).

false target repeater – A deception jammer that receives a signal, alters that signal in a specified fashion, and retransmits the false signal.

fast sweep jamming – Jamming accomplished by a transmitter that is rapidly tuned or swept over a broad frequency range.

fast-time-constant (ftc) techniques – Fast-time-constant radar signal processing techniques used to reduce the effects of certain types of undesired signals and ECM.

feedback systems – Feedback ECCM systems employ the tactic of adjusting system parameters in accordance with the conditions of the link. If, for example, noise is high, the data rate is reduced by repeating the message. Other adjustments in the circuits can be made to compensate for bad transmission conditions. Channel monitoring also can be used to tell when the link is clear.

ferret – An aircraft, ship, or vehicle especially equipped for detecting, locating, recording, and analyzing electromagnetic radiation.

filbert – A kite balloon, with a corner reflector suspended inside, that can be flown from a ship or float.

flare – A type of pyrotechnic decoy used against ir-seeking devices.

flash blindness – Temporary or permanent impairment of vision resulting from an intense flash of light. It includes loss of night adaptation and dazzle, and may be associated with retinal burns.

frequency agility – The capability of an EW system of rapidly changing frequency of transmission within the limits of its operation range.

frequency-hoppers – Frequency-hopper systems usually employ frequency synthesizers that are hopped over a given spectrum in a random fashion. Systems can have one frequency shift per information bit or any number of shifts. The net effect is to spread the information over a wider bandwidth, reducing the effectiveness of a given noise jammer and adding protection against deception ECM. Processing gain for such systems generally is taken as the ratio of the total frequency range hopped to the information bandwidth.

frequency time dodging – As a complement to frequency-hopping, a "time dodging" receiver can be gated on at the precise instant and frequency that data are expected.

G

guarded frequency – *See:* **restricted frequency.**

gulls – A reflector device near ground or water level used in electronic countermeasures.

gulls jamming – This jamming signal is generated by a quick rise and slow fall of a variable audio frequency. Nuisance effect on voice-modulated circuits.

H

harp material – Generally, a coating or layer of material that absorbs radar energy. Used for the radar camouflage of targets.

home-on-jam – An adaptation of active or semiactive guidance systems to give them a homing guidance system capability when their normal guidance capability is disrupted by jamming.

hunt-lockon jammer – See: **automatic search jammer.**

I

image jamming – Jamming accomplished by jamming on the image frequencies.

imitative electronic deception – The intrusion on the enemy's channels and the introduction of matter in imitation of his own electromagnetic radiations for the purpose of deceiving or confusing him. *See also:* **electronic deception** and **manipulative electronic deception.**

infrared counter-countermeasures (IRCCM) – Actions taken to employ effectively our own infrared equipment and systems in spite of the enemy's actions to counter their use.

infrared countermeasures (IRCM) – The actions taken to prevent or reduce the effectiveness of enemy infrared equipment and tactics.

instantaneous automatic gain control (iagc) – An anticlutter method, used in radar, that lowers the gain promptly on receipt of strong echoes or interference.

interceptibility – In electronic warfare interceptibility refers to the degree to which a signal of interest can be detected and recognized. Detection and recognition imply that some minimum measure of signal parameters must be made—for example, frequency, pulse repetition rate, pulse width, bandwidth, modulation characteristics, and scan characteristics. The information derived from the intercept of electromagnetic signals may form the basis for taking some future action or it may be used as a basis for some immediate operation.

interception – The act of listening in on and/or recording signals intended for another party for the purpose of obtaining intelligence.

intercept receiver – A receiver designed to detect and provide visual and/or aural indications of electromagnetic emissions occurring within the particular portion of the electromagnetic spectrum to which it is tuned.

interference – Any electrical disturbance to equipment that causes undesirable responses in electronic circuits.

intrusion – The transmission of content, symbols, headings, etc., to interfere with or harass enemy communications in such a way that the enemy recognizes the source as nonfriendly to him.

J

jamming – The deliberate radiation, reradiation, or reflection of electromagnetic signals with the object of impairing the use of electronic devices, equipment, or systems being used by an agressor.

jamming-to-signal ratio (J/S) – The ratio of the jamming signal power to the target signal power measured at the target receiver antenna, receiver input, if, or video terminals.

K

keyed cw jamming – A jamming method employing an unmodulated continuous wave that is keyed (interrupted) either randomly or with Morse code characters.

kite – A reflection device suspended high in the air; used in electronic countermeasures.

L

lockon – Signifies that a tracking or target-seeking system is continuously and automatically tracking a target in one or more coordinates (e.g., range, bearing, elevation).

lookthrough – A technique whereby the jamming emission is interrupted irregularly for extremely short periods to allow monitoring of the victim signal during jamming operations.

M

mainlobe jamming – Jamming through the mainlobe of the victim's receiving antenna.

manipulative electronic deception (med) – The use of friendly electromagnetic radiations in such a manner as to falsify the information that a foreign nation can obtain from analysis of these electromagnetic radiations.

masking – The use of electromagnetic radiation, chaff, or aerosols to conceal a particular electromagnetic radiation as to location of source and/or purpose of the radiation; also referred to as screen jamming.

meaconing – A system of receiving beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings to be obtained by the enemy aircraft or ground stations. Meaconing also refers to placing beacon signals in "false" positions.

monopulse jamming – Retransmitting the monopulse signal with a phase shift to cause the radar tracking system to pull completely off the target. Also known as "cross-eye" jamming.

mutual screening – The protection of a unit not having a jamming capability by a unit that does have a jamming capability.

N

noise jamming – Electronic jamming in which the carrier wave is modulated by noise.

noncommunication jamming (noncomjam) – Jamming used against devices other than those used as a means of communication. Typical noncomjam targets are navigation aids, radars, guidance systems, and proximity fuzes.

O

off-frequency spot jamming – A technique of jamming with a narrowband or spot jammer in which the spot jamming is not on the transmission frequency of the radar but still is within the receiver bandwidth of the radar.

off-target jamming – The employment of a jammer at a point removed from the main units of the force to defeat the enemy's use of our jamming signals to his advantage.

optical countermeasures (OCM) – The use of optical radiation to deny or minimize the use of victim optical device.

opto-electronic countermeasures (OECM) – The use of radiation in the optical wavelengths, which ultimately affects the electronic circuitry of the victim system.

optical support measures (OSM) – The use of nonelectronic optical support measures such as the use of ordinary binoculars.

P

padding – Words or phrases, unrelated to the text of a message, added prior to encryption and deleted upon decryption, or addition of random code groups to increase group count.

penetration aids (penaids) – Electronic systems, in particular avionic systems, that aid an aircraft in penetrating a hostile electronic air defense envelope. Penaids may consist of ESM and ECM instruments.

protected frequency – *See:* **restricted frequency.**

pseudorandom ECCM systems – In pseudorandom systems, a pseudorandom-code generator is used to produce a long random-bit sequence. The same sequence is available in the receiver. When transmission starts, the two code generators are synchronized. Information bits then are expanded into the random code stream in a one-to-many transformation. Correlation processing is used in the receiver to identify the incoming sequence as a one or zero. This system can be used for data systems or digitized voice.

pulse deception or jamming – A technique of deception jamming in which pulses are generated by the jammer that are similar to the reflected signals from the target or data signals in digital data systems. The pulses can be made to appear at other ranges and azimuths than those of the true target.

R

radar camouflage – Concealing the presence or the nature of an object from radar detection by the use of coverings or surfaces that considerably reduce the radio energy reflected toward a radar; i.e., radar-absorbent materials.

radar intelligence (radint) – *1.* Intelligence concerning radar, or intelligence derived from the use of radar equipment. *2.* Organization or activity that deals with such intelligence. (Note: In sense 1, the term radar intelligence has been used with several specific meanings; these are (a) that aspect of electronic intelligence that deals with radar; (b) intelligence concerning the radar aspects of a radar mission, especially a radar-bombing mission, radar target intelligence; and (c) intelligence derived from information procured by means of radar, particularly with regard to bomb damage assessment and bomb scoring.)

radio direction finding – Radio location in which only the direction of a station is determined by means of its emissions.

radio fix – The location of a friendly or enemy radio transmitter, determined by finding the direction of the radio transmitter from three or more direction finding stations.

railing – In electronics, radar pulse jamming at high recurrence rates (50 to 150 kHz), resulting in an image on a radar indicator resembling fence railings.

random-keyed cw jamming – Jamming through the keying (interrupting) of an unmodulated radio frequency carrier at a random rate. Used to jam radio teletype-

writer, radiofacsimile, and radiotelegraph (cw) circuits.

random noise jamming – Synthetic noise that is random in amplitude and frequency. It is similar to normal background noise.

random pulse jamming – Jamming technique wherein random pulses are transmitted at irregular rates.

range-angle repeater – A repeater jammer that combines both range deception and angle deception jamming against tracking radars.

range gate stealer – A type of repeater jammer designed to capture a radar range gate, thus causing the radar to disrupt its tracking function.

receiver blanking – Receiver blankers detect the presence of an interfering signal of large magnitude (a spike) and turn the receiver off until the interference has diminished. The technique is particularly effective against pulse jamming.

reflective jamming – Use of radar confusion reflectors to return false and confusing signals to the enemy radar receiver.

repeater jammer – Jamming system that receives a target signal, amplifies and modifies it, and retransmits it back to the source, causing errors in the data obtained from the radar.

restricted frequency – A frequency against which intentional jamming or other forms of interference is prohibited.

rope – An element of chaff consisting of a long roll of metallic foil or wire, which is designed for broad, low-frequency response.

rotary jamming – This signal is a low-pitched, slowly varying audio frequency. Effective against voice-modulated circuits.

S

screen jamming – *See:* **masking.**

search receiver – A special receiver that can be tuned over a relatively wide frequency range in order to detect and measure electromagnetic signals transmitted by the enemy.

self-screening – The protection of a unit by means of a self-contained jamming capability.

sequential spot jammer – A spot jammer that automatically tracks and jams on the frequency of detected signals.

sidelobe blanking – A technique that compares relative signal strengths between an omnidirectional antenna and the radar antenna. Used to prevent unwanted signals at false azimuths from entering the detection circuits.

sidelobe cancellation – A jamming countermeasure technique that is designed to exclude or greatly reduce the strength of jamming signals introduced through the sidelobes or backlobes of a receiving system.

sidelobe jamming – Jamming through the sidelobes of the victim's receiving antenna.

signal intelligence (sigint) – A generic term that includes both communication and electronic intelligence.

signal security (sigsec) – A generic term that includes both communication and electronic security.

signature – The characteristic pattern of the target displayed by detection and identification equipment.

skirt frequency jamming – A form of off-frequency jamming in which effectiveness depends upon imbalances between sum and

difference channels where rapid phase shifts are occurring.

slip coating – Chemical film applied to chaff dipoles to reduce clumping together (birdnesting) of the dipoles.

spark jamming – A burst of noise of short duration and high intensity that is repeated at a rapid rate. Effective against all types of radio communications.

spoiling – The process whereby spurious synchronized transmitters add to the service coverage of a system reducing or nullifying the value of the system as a navigational aid. Similar to meaconing.

spoofing – A deception technique to create false targets on a victim display or indicator.

spot jamming – The jamming of a specific channel or frequency.

stepped tone jamming – Sometimes called bagpipes, the signal consists of separate audio tones in varying pitch. Effective against fm and am radios.

susceptibility – The degree to which a device, equipment, or weapon system is open to effective attack because of one or more inherent weaknesses.

sweep jammer – A transmitter that emits a jamming signal consisting of a carrier wave (unmodulated or modulated) whose frequency is varied continuously within a given bandwidth.

sweep lockon jamming – A jamming system that sweeps a wide range of frequencies with a receiver. When a signal is detected, the sweep stops and the transmitter is activated.

synchronized pulse jamming – A jamming technique wherein jamming pulses are timed to arrive at the receiver when the receiver gate is open.

T

taboo frequency – *See:* **restricted frequency.**

turnstiles – A confusion reflector device consisting of three mutually perpendicular linear metallic elements.

U

unintentional radiations – Spurious electrical, magnetic, and acoustical impulses that are emitted when electrical and electronic systems not intended to radiate are placed in operation.

V

velocity gate pull-off repeater – A repeater that steals the velocity gate of pulse Doppler radars by shifting frequency of the repeated signals.

vulnerabilities – The characteristics of a system which cause it to suffer a definite degradation (incapability to perform designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) environment.

W

window – Strips of frequency-cut metal foil, wire, or bars; usually dropped from aircraft or expelled from projectiles or rockets as a radar countermeasure.

wobbler jamming – This jamming signal is a signal frequency modulated by a low and slowly varying tone. Nuisance effect against voice-modulated radio circuits.

BIBLIOGRAPHY

(U) ARMY REGULATIONS

AR 11-13 *Army Electromagnetic Compatibility Program* (U), 29 July 1969. (UNCLASSIFIED publication)

AR 105-2 *Electronic Counter-countermeasures (ECCM)* (U), 29 August 1973. (CONFIDENTIAL publication)

AR 105-3 *Reporting Meaconing, Intrusion, Jamming, and Interference of Electromagnetic Systems* (U), 13 March 1972. (CONFIDENTIAL publication)

AR 105-5 *Electromagnetic Cover and Deception (EC&D)* (U), 9 July 1973. (CONFIDENTIAL publication)

AR 105-87 *Electronic Warfare (ESM, ECM, ECCM)* (U), 29 November 1973. (CONFIDENTIAL publication)

AR 381-19 *Requests for Intelligence Support* (U), 22 August 1974. (UNCLASSIFIED) publication)

(U) FIELD MANUALS

FM 32-5 *Signal Security (SIGSEC)* (U), 26 June 1970. (CONFIDENTIAL publication)

FM 32-6 *SIGSEC Techniques* (U); 10 July 1972. (UNCLASSIFIED publication)

FM 32-15 *Broadcast Countermeasures* (U), 1 June 1966. (SECRET publication)

FM 32-20 *Electronic Warfare* (U), 14 September 1971. (CONFIDENTIAL publication)

FM 32-20-1 *Electronic Countermeasures Handbook* (U), October 1971. (SECRET publication)

(U) HANDBOOKS

Foreign Intelligence Office Handbook (U), AMC, July 1973. (UNCLASSIFIED publication)

(U) TEXTBOOKS

Fundamentals of Electronic Warfare, US Air Force Academy, 1 March 1972.

(S) CHAPTER 2

GENERAL APPROACH TO VULNERABILITY OF COMMUNICATION-ELECTRONIC AND ELECTRO-OPTICAL SYSTEMS TO ELECTRONIC WARFARE (U)

LIST OF ABBREVIATIONS

ABBRE-VIATION	DEFINITION
ACCESS	ASA Computer-Controlled Environmental Simulation
ALGOL	an international algorithmic language
AMCN	Analytical Model of a Communications Network
ARTSS	ARMATS Real-Time Systems Simulator
CAA	combined arms army
CDC	Control Data Corporation
CE	Communication-electronic
C/I	carrier-to-interference ratio
CIL	Common Intelligence Language
cm/cb	countermortar/counterbattery
C/N	carrier-to-noise ratio
COMINT	Communications Intelligence
COMMEL	Communications-Electronics
CRESS	Combined Reconnaissance, Surveillance, and SIGINT
df	direction finding (er)
ECC	European Communist Countries
ECCM	electronic counter-countermeasures
ECM	electronic countermeasures
elint	electronic intelligence
em	electromagnetic
EMETF	Electromagnetic Environmental Test Facility (US Army)
EO	electro-optics
ESM	electronic support measures
ESSA	Environmental Science Services Administration
EW	electronic warfare
fax	facsimile
feba	forward edge of the battle area
FIO	Foreign Intelligence Officer
flir	forward-looking infrared
FORTRAN	programming language for problems expressed in algebraic notation
GHz	gigahertz (10^9 hertz)
hf	high frequency (radio) (3-30 MHz)
IBM	International Business Machines Corporation

if	intermediate frequency
ir	infrared
JCS	Joint Chiefs of Staff
kHz	kilohertz (10^3 hertz)
km	kilometer
MASS	Mallard Simulating Set
mf	medium frequency (radio) (300 kHz-3 MHz)
MHz	megahertz (10^6 hertz)
NA	not applicable
NATO	North Atlantic Treaty Organization
NBS	National Bureau of Standards
nir	near infrared
OW	optical warfare
rf	radio frequency
SATCOM	communications (relay) satellite
SE	system effectiveness
sigin	signal intelligence
S/N	signal-to-noise ratio
soj	standoff jammer
TA	tank army
taray	target array
TRADOC	Training and Doctrine Command
UDF	User Data File
uhf	ultrahigh frequency (radio) (300 MHz-3 GHz)
USAEPG	US Army Electronic Proving Ground
vhf	very high frequency (radio) (30-300 MHz)

LIST OF SYMBOLS

A = accessibility, dimensionless

d_j = distance between the ECM victim and the ECM source, km

d_t = distance between the ECM victim and the legitimate signal source, km

F = feasibility, dimensionless

i = subscript designation for an ESM site, –

I = interceptibility, dimensionless

j = subscript designation for an ECM source, –

S = susceptibility, dimensionless

t = subscript designation for a legitimate transmitting source, –

v = subscript designation for the ECM victim, –

V = vulnerability, dimensionless

Δh = terrain roughness factor, m

θ = direction angle of the victim antenna with respect to the ECM source, deg

 = map symbol representing ECM victim sensor site or legitimate transmitting site (site passing bonafide traffic to the ECM victim), –

 = map symbol representing an ESM site, –

 = map symbol representing an ECM site, –

2-1 (U) INTRODUCTION

The purpose of this chapter is to provide the design engineer with basic concepts and background information regarding EW vulnerability analysis and to provide a point of reference or point of departure for the chapters of this handbook covering the vulnerability of communication-electronic (CE) and electro-optical (EO) systems to EW.

The purpose of vulnerability analysis is threefold:

(1) To determine the ability of CE and EO systems to perform their missions satisfactorily in a hostile EW environment. This determination requires theoretical analysis and laboratory field tests, as well as operational tests conducted under as realistic an EW threat environment as possible.

(2) To determine system design modifications required to maintain minimum performance standards.

(3) To determine the type of training and techniques required by operational personnel to work through EW attacks.

2-2 (U) THE PHILOSOPHY OF VULNERABILITY TO ELECTRONIC WARFARE

2-2.1 (U) PERSPECTIVE

Vulnerability, as defined by JCS Publication 1 (Ref. 1), "is the characteristics of a system* which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment."

Three general elaborations of this definition can be made:

a. A vulnerable system has inherent weaknesses that make it potentially liable to definite degradation by deliberate enemy action.

b. A given enemy or threat force has a capability in being or has the technical know-how and resources to develop a capability that can degrade the system.

c. The degradation takes place in an active operational setting (real or simulated), and both the subject system (victim) and the enemy (threat countering) system are tactically situated and operating in accordance with their respective doctrine and modus operandi.

It follows then that vulnerability to EW, as used in this handbook, is a measure of the capability, stated in the form of a probability, if possible, of a given CE or EO system to perform effectively in the face of hostile EW actions. Vulnerability to EW of a given CE or EO system includes such factors as (a) the probability of an ECM attack and the sensitivity to ECM effects, (b) the probability of signal intercept and the ESM signal exploitation effects, and (c) the nature and scope of the hostile EW threat (Ref. 2).

Determination of vulnerabilities to EW of all systems dependent upon electromagnetic radiation is necessary at an early phase in the developmental cycle so that appropriate decisions can be made regarding:

a. The need for the development of electronic counter-countermeasure (ECCM) circuits or procedures

b. The desirability of continuing with the development of the system

c. The impact on budgetary resources

d. Personnel and training requirements.

2-2.2 (U) THE PRIMARY FACTORS OF EW VULNERABILITY EVALUATION

The determination of vulnerability to electronic warfare is a process of evaluation. This

*A system is an organized collection of men, machines, and methods to accomplish a specific objective.

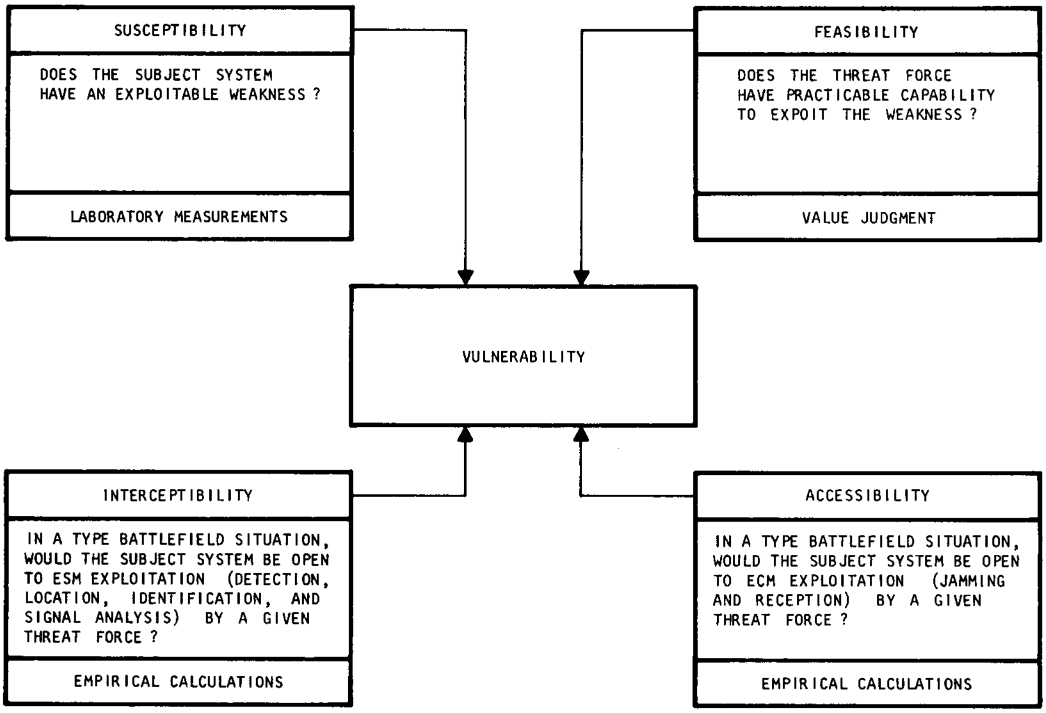


Fig. 2-1 (U). The Primary Factors of Vulnerability Analysis (U)

process of evaluation involves the investigation of four sets of factors or elements: susceptibility, interceptibility, accessibility, and feasibility (Ref. 3). The relationship among these elements is illustrated in Fig. 2-1.

a. *Susceptibility.* EW susceptibility is the degree to which a system is open to degradation by a deliberate EW attack. It pertains to the effect of an interfering signal upon the acceptable performance of a given CE or EO system. A system designed to respond to a certain category of signals transmitted by a desired source most likely will respond also to similar signals transmitted from an undesired source as well as to some dissimilar systems. From the total point of view of vulnerability, this undesirable situation can be minimized through circuit design, operator training, and good operational practices. From the narrow point of view of susceptibility, this undesirable feature can only be minimized through circuit design and is measured under laboratory or laboratory-like conditions. One of the purposes of the laboratory tests is to determine and to quantify the threshold of minimum performance characteristics (determining the thresholds of susceptibility). Another is to determine the amount of degradation for various interference-to-signal ratios from no degradation to "maximum" degradation (i.e., the threshold of susceptibility).

A most important element in this step is the development of criteria. An ideal criterion would be a quantified threshold, such as a definable measure of jamming power and modulation for a given signal level, that at some level would prevent the system from carrying out a specific objective. The development of good criteria is a most difficult task. Value or subjective judgment criteria must be avoided. As a minimum, criteria must be established that satisfy the following:

(1) What is the effect of introducing various interfering signals into a system receiver?

(2) Can significant degradations of system performance be achieved by injection of internal intentional interference?

(3) How do system errors relate to interference levels?

(4) Is there an optimum interfering signal from the standpoint of a jammer?

b. *Interceptibility*. EW interceptibility is the likelihood, or statement of probability, that an enemy EW system could detect and locate the system under consideration and exploit the radiated signals for the purpose of mounting and executing an EW attack. Interceptibility analyses and tests are conducted to determine (1) the probability of intercepting signals emanating from the system, (2) the probability of locating the system by EW means, and (3) the amount and type of information that may be revealed to the enemy. In particular, this includes information that the enemy may use to the detriment of the using agency and other friendly forces. An important element, as in all other steps of vulnerability analysis, is the development of meaningful criteria. Questions relating to interceptibility determination should include, as a minimum, the following:

(1) Can the signal transmissions emanating from the victim systems be intercepted by EW means?

(2) In what deployment situations can intercept be achieved?

(3) What signal parameters can be determined through intercept?

(4) Which of the above signal parameters are essential to the conduct of an EW attack by the enemy?

c. *Accessibility*. EW accessibility is the likelihood, or statement of probability, than an enemy EW (jamming and deception) system could couple with the victim system and cause the victim system to fail to perform satisfactorily. Jamming and deception tests are conducted to determine how the operational capability of the victim system is affected while it is operating under an EW attack. These tests may be operational and may be made under simulated combat conditions (computer assisted simulation tests and/or field exercise). In most cases, interceptibility tests and accessibility tests will be conducted together. Here again an important element is the development and selection of meaningful criteria. Questions pertaining to accessibility determination should include among others the following:

(1) What are the points in the system that are open to a threat jamming and/or deception attack?

(2) How are the above points of access affected by antenna patterns, geography, deployment geometry (siting, etc.), propagation factors, and operating methods?

(3) Can accessibility be minimized by approaches such as equipment siting, other operating procedures, or specialized training of user personnel?

d. *Feasibility*. EW feasibility is the likelihood, or statement of probability, that a threat system of definitive parameters can be developed by a potential enemy and will be targeted against the victim systems. The concept of EW feasibility is far-reaching and, therefore, can be very ambiguous. It not only pertains to that which is in existence but also to that which may be possible in the future. EW feasibility applies to a threat that has not been observed in being, but that all available indicators strongly suggest could be developed and fielded. EW feasibility encompasses a myriad of things technical, economic, and geopolitical, as well as tactical. It is by far the least scientific evaluation factor in EW vulnerability determination. Feasibility represents the set of parameters having the largest uncertainty of estimate and widest margin of

error. EW feasibility to a large degree is a value judgment* involving both the engineer and the intelligence analyst.

The preceding factors of feasibility include, among other things:

(1) Geopolitical factors–perhaps the most significant being retaliation. For example, there is the notion of "hands-off" doctrine, e.g., I will not interfere with your operation if you do not interfere with my operation. Perhaps diplomatic and commercial traffic via SATCOM means may well fall within this category. Or perhaps some categories of military traffic may also fall within the general limits of the "hands-off" doctrine.

(2) Technological factors–the engineering know-how and the possession of the facilities necessary to develop and manufacture an effective EW system.

(3) Economic factors–the men, money, and material resources necessary to develop and procure the system and to operate, maintain, and support the system in the field.

(4) Tactical factors–the operational considerations such as employment/deployment, flexibility and mobility, command and control problems, the overall contribution to the success in battle, and last, but not least, the self-inflicted penalties incurred by the EW attacking force. Penalties such as (a) interference to the attacking forces' own command and control communications, intelligence-gathering operations, and control of supporting weapons; (b) the revelations of sophisticated knowledge gained through the study and exploitation of intercepted signals; and (c) the likelihood of drawing suppressive fire and other forms of physical retaliation.

*A value judgment, as opposed to a fact judgment, centers around the notion of verifiability. In a fact judgment such things as setting a limit of acceptibility can be quantified, measured, and verified. In a value judgment, it is virtually impossible to set a limit and to quantify, measure, and verify it. For example, it is extremely difficult to determine what is or is not economically feasible to an enemy threat force.

Given that a particular set is susceptible, can be intercepted, and is accessible to a jamming and deception threat, that the estimate of the threat's state of the art indicates that there is a demonstrated EW capability, and that there are no adverse geopolitical or tactical factors, the critical question of feasibility centers around the following:

(1) Is it cost-effective to the enemy or threat forces to employ EW against the subject CE or EO system?

(2) Is it realistic militarily for the enemy or threat force to employ EW against the subject CE or EO system?

2-2.3 (U) TECHNICAL AND OPERATIONAL VULNERABILITY ANALYSIS

2-2.3.1 (U) General

Vulnerability V to EW may be expressed as a function of susceptibility S, interceptibility I, accessibility A, and feasibility F (Ref. 4).

$$V = f(S, I, A, F) \tag{2-1}$$

where

S = the set of EW susceptibilities derived from laboratory measurements

I = ESM interceptibility assessments derived from empirical evaluation or simulations

A = ECM accessibility assessment derived from empirical evaluation or simulations

F = EW environment feasibility derived from extrinsic factors (see par. 2-2.2.d). The F parameter, as noted in par. 2-2.2.d, is difficult to quantify and to combine with other assessments so that meaningful and quantifiable answers can be provided.

A flow diagram showing the relationship of susceptibility, interceptibility, accessibility, and feasibility and their interaction with the intrinsic factors associated with EW vulnerability analysis is shown in Fig. 2-2. Because of the broad scope of EW vulnerability analysis, for purposes of this handbook EW Vulnerability Analysis is subdivided into two parts: Technical EW Vulnerability Analysis and Operational EW Vulnerability Analysis. The design engineer is concerned primarily with technical EW vulnerability analysis; however, he must be aware of the impact of operational factors upon the design of his system.

2-2.3.2 (U) Distinctions Between Technical EW Vulnerability Analysis and Operational EW Vulnerability Analysis

Technical vulnerability is concerned primarily with the technical aspects of susceptibility*, accessibility, interceptibility, and feasibility. Operational vulnerability* assessments consider not only these factors but also tactics; i.e., employment and deployment of the friendly electronic system as well as the employment and deployment of the enemy EW system. Technical and operational vulnerability assessments require both theoretical analyses and testing. Some distinguishing features are:

a. Technical vulnerability tests usually are conducted under instrumented range conditions and usually involve a static EW threat. Operational vulnerability tests are conducted under "tactical" conditions and usually involve a dynamic EW threat (EW aggressor elements).

b. Technical vulnerability tests provide information concerning the technical or engineering adequacy or inadequacy of the equipment being evaluated, whereas operational vulnerability tests provide technical information on the overall functional effectiveness of the equipment in a simulated combat environment.

c. Technical vulnerability analyses and tests are conducted throughout the developmental cycle. Operational vulnerability tests, except for the computer-assisted simulation exercise, usually are conducted near the end of the development cycle. Both technical and operational analyses and testing are essential to the EW vulnerability evaluation process. Technical vulnerability evaluation testing is much more scientific and precise than operational evaluation. However, the value of a system as a military instrument of combat can better be derived from thorough operational testing.

2-2.3.3 (U) Technical EW Vulnerability

Technical EW vulnerability is a primary concern of the design engineer. It is imperative that technical EW vulnerability considerations be included in all phases of the developmental cycle. Technical EW vulnerability is an indication of the capability of a given CE or EO system of operating effectively in a specified EW environment. A simplified flow diagram illustrating technical EW vulnerability analysis is shown in Fig. 2-3. See par. 2-2.2 for a discussion of the four primary factors of EW evaluation. In the main, the design engineer is concerned with establishing the limits or bounds of susceptibility, the conduct of technical interceptibility and accessibility tests, and the preparation of technical findings and conclusions. Although feasibility is a critical factor in the formulation of valid findings and conclusions, the feasibility task is primarily one of intelligence. The design engineer is concerned primarily with minimizing the susceptibility, the probability of intercept

*In some Army publications the terms susceptibility and vulnerability take on the same meaning as those defined in this handbook as technical vulnerability and operational vulnerability, respectively. The term susceptibility occasionally is used by engineers to connote technical vulnerability, and the term vulnerability is used to connote operational vulnerability

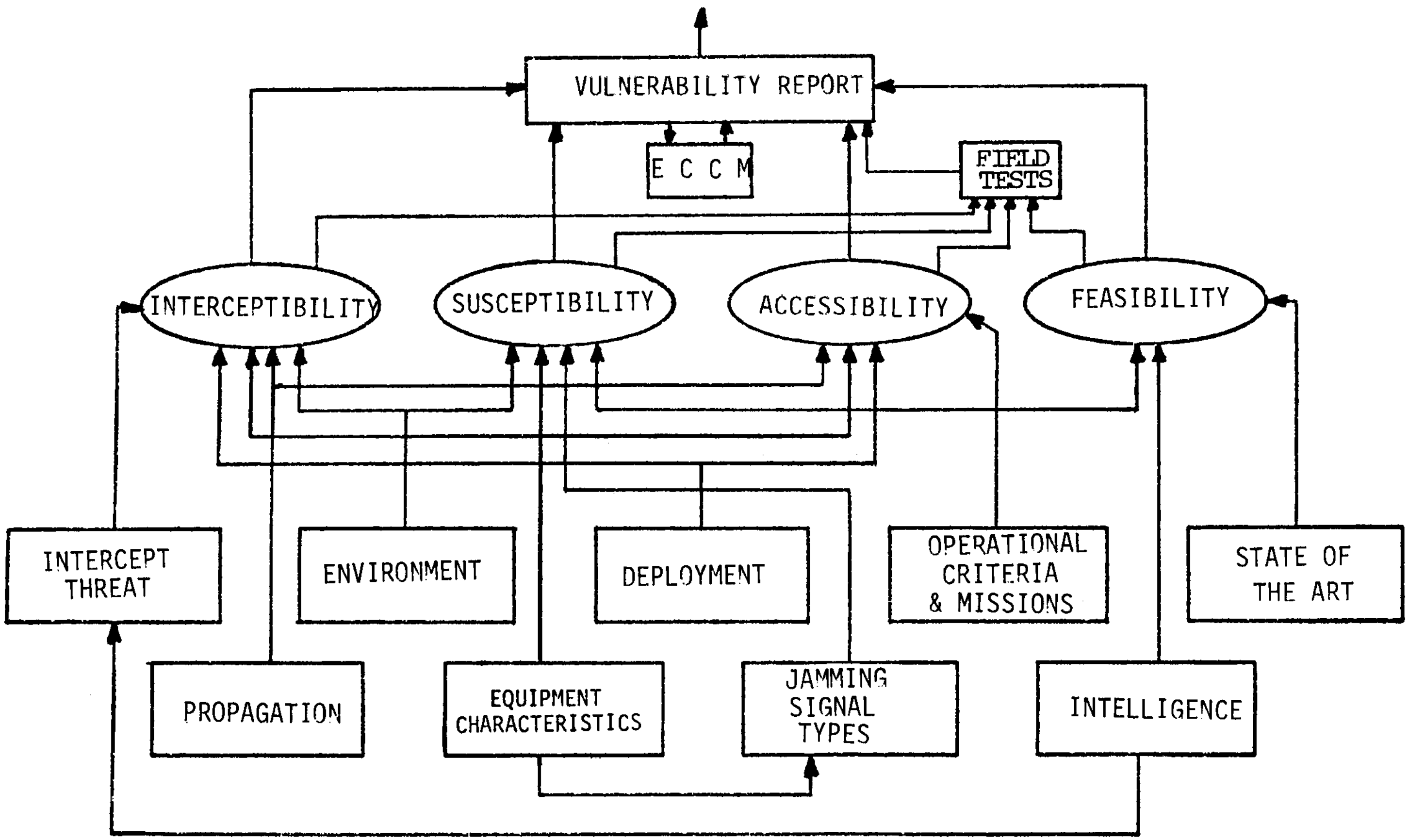


Fig. 2-2 (U). Flow Diagram of EW Vulnerability Analysis (U)

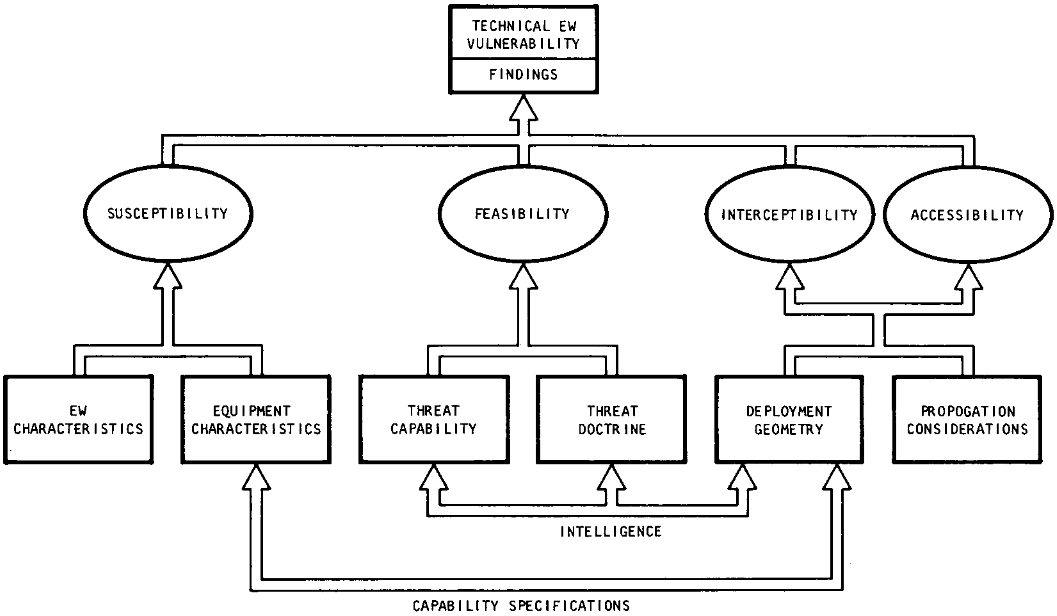


Fig. 2-3 (U). Flow Diagram of Technical EW Vulnerability Analysis (U)

to include detection, location, and signal exploitation and to minimize the accessibility of a set or system to ECM. Technical EW vulnerability evaluations can be made by thorough test and analysis, computer-assisted simulation analysis, or a combination of the two. The process Technical EW Vulnerability analysis by computer assistance requires the use of detailed models (see par. 2-4). In field evaluation the design engineer must consider, in addition to technical factors, such things as the appropriate deployment geometry and the geometric relationships between threat EW systems and victim system and legitimate signal source.* (See Fig. 2-4.)

*In EW calculations and EW geometric diagrams, map arrays, etc., it is customary to use the symbol or a subscript i to represent an ESM site. An ESM target is represented by the symbol or a subscrpt t. In ECM the symbol is used to represent both the victim and the rf source which is sending or transmitting the legitimate signal energy received by the victim. The subscript for the victim is usually v or r. The subscript for the signal source is t. In ECM the victim is the electromagnetic sensor or receiver which is being or is to be encountered. The symbol for ECM source is and the subscript designation is j. The designator d_t is the distance between the victim and the transmitter source and d_j is the distance between the victim and the ECM source. The angle θ is the victim antenna orientation with respect to the ECM source.

The geometric relationship also includes antenna orientation, propagation path considerations, and power/distance considerations. See also the discussions included in Chapters 3 through 7 for details relating to EW vulnerability analysis of generic CE and EO systems.

2-3 (S) EW THREAT PRECEPTS

2-3.1 (U) GENERAL

The purpose of this paragraph is to present a preview of the EW effort of the Warsaw Pact forces in general and to outline the basic EW precepts relating to the Soviet effort in particular. Further details relating to a specific threat are included in Appendix B, Chapters 3 through 7. Because of the changing nature of threat parameters, the design engineer should always check with his Foreign Intelligence Officer (FIO)** to assure himself that he is using the most recent threat information.

**See par. 1-3 for details pertaining to the FIO concept.

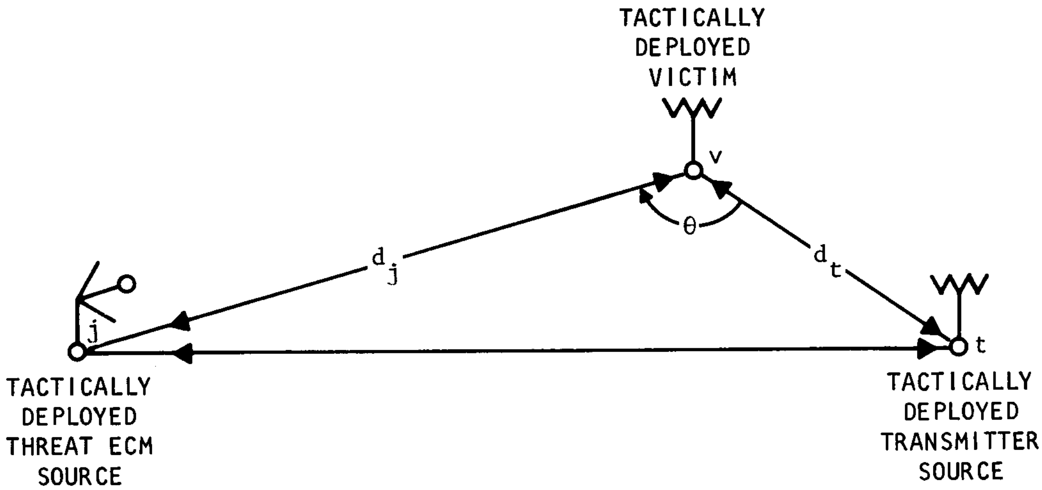


Fig. 2-4 (U). Diagram Illustrating Geometry of ECM Vulnerability Analysis (U)

2-3.2 (S) EW THREAT

The European Communist Countries (ECC) in general and the USSR in particular have one of the most sophisticated and extensive EW capabilities in the world. Soviet experience in comint dates from the reorganization of the Red Army in the early twenties. Their experience in elint and ECM dates from World War II. Electronic warfare planning within the Soviet hegemony is done by the Chief, Operations Directorate, of the Ministry of Defense and the formation levels (e.g., Army front and similar organizational levels), as illustrated in Fig. 2-5. The coordination and control of EW is rigid. Fig. 2-6 is a level-of-effort diagram of a typical signal intercept/ECM capability of a Warsaw Pact country. A typical Warsaw Pact army front is expected to have five or six ground armies—with about a 2:1 ratio of combined arms armies (CAA) to tank armies (TA)—and a tactical air army (TAA). A typical ground army of four combat-maneuver divisions has an overall signal intercept capability of 24 hf radio-intercept positions, 28 vhf/uhf radio intercept positions, eight hf radio df positions, 12 vhf radio df positions, 12 radar df positions, and 17 radar intercept positions.

The Warsaw Pact nations are attributed with an ECM capability of 12 vhf communication jamming positions, six hf communication jamming positions, and four vhf ESM/df positions. At least 60 percent of these positions are expected to be situated within 8 km from the forward edge of the battle area (feba). These forward-area positions will be targeted against battlefield surveillance radars and division communications.

2-3.3 (S) TACTICAL SIGINT/ESM

The Soviets, fully aware of the positive values of signal intelligence (sigint)/ESM, consider information derived from analysis of enemy CE emanations to be a lucrative source of combat information. The basic EW mission of the tactical sigint/ESM units is to derive electronic-order-of-battle (eob) and EW target data. Warsaw Pact army and division-level signal collection units most likely will cover enemy (NATO) operational activities occurring within their immediate zone of influence. Deeper collection probes are expected to be made by front and tactical air collection elements.

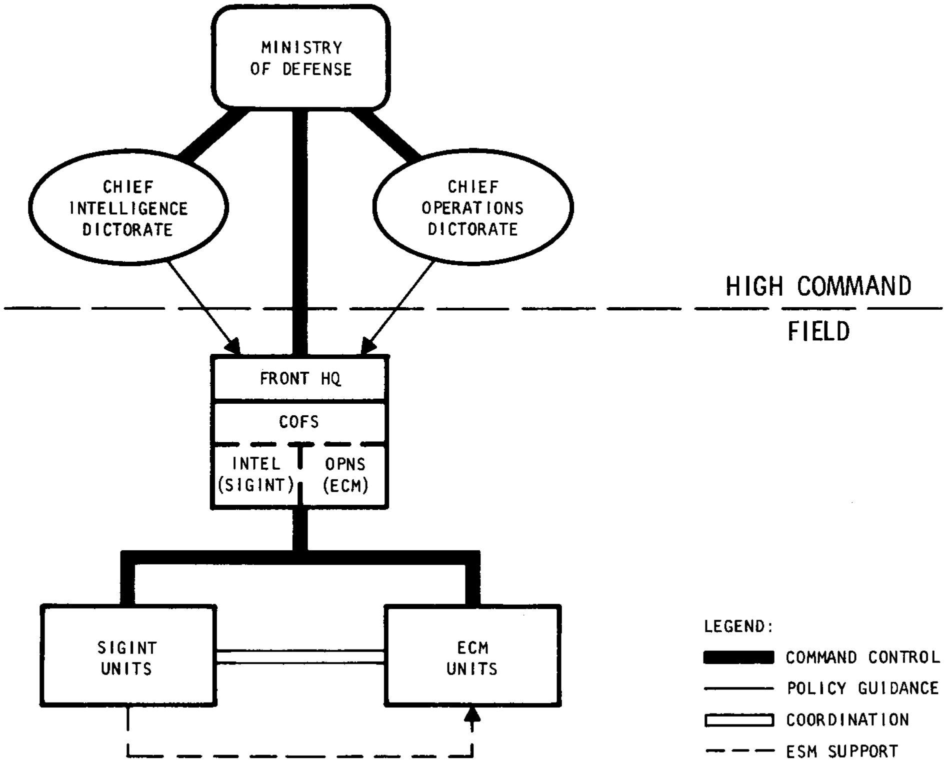


Fig. 2-5 (S). Postulated Mechanism for Control and Coordination of Soviet EW Operations (U)

2-3.4 (C) TACTICAL ECM

The element of surprise is the fundamental principle of ECM commitment. ECM is expected to be used as a weapon against clearly defined targets. It is estimated that by the late seventies or early eighties, the Warsaw Pact forces will have a capability for countering 8 to 10 forward-area nets of a given NATO division. Warsaw Pact forces in recent exercises have clearly indicated that a typical EW attack will include rf jamming, chaff, and drops. In this connection, it appears that a rocket-delivered chaff attack against targets such as countermortar/counterbattery (cm/cb) radar is much more likely than the conventional rf attack. Rf illumination by standoff jammers (soj) does, however, appear likely. The Warsaw Pact forces also are skilled in the art of imitative deception and traffic intrusion, in particular, planned traffic intrusion and the use of bogus signals.

2-3.5 (S) TACTICAL ELECTRO-OPTICAL WARFARE*

During World War II the Soviets were hurt by German use of tactical near-infrared (nir) devices. They learned their lesson and started to investigate these systems and their capability immediately after the war. Since the Soviets have stressed night fighting, their early tactical concepts called for neutralization of enemy (NATO) night vision devices by weapon fire and lights such as searchlights and flares. Success of US systems such as ir scanners, flir's, and laser-guided weapons during the Vietnam conflict has further demonstrated the tactical value of these devices, which in turn demands suitable countermeasures.

*See also par. 6-2.3 for details relating to the optical threat parameters.

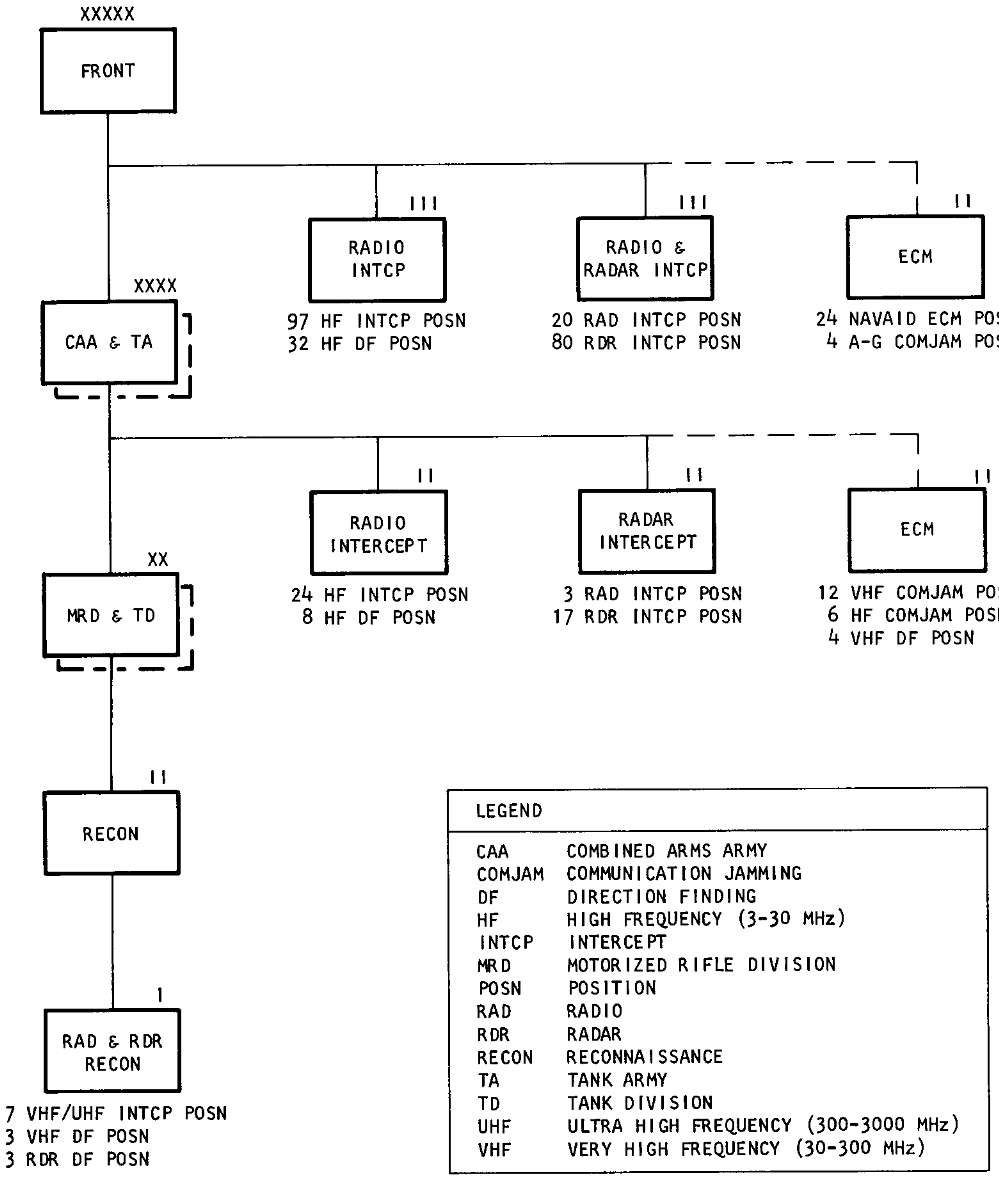


Fig. 2-6 (S). Diagram of a Typical Warsaw Pact Signal Intercept/ECM Capability (U)

In contrast to the intent and capability for EW that exists in the rf region, no definitive intent nor capability for EW has been demonstrated or observed in the optical region. This should not be interpreted to mean that such intent does not exist, but rather that the technology for such optical warfare devices is fairly new and advancements are concealed rather easily. Optical systems inherently do not radiate over anywhere near as large a range as do microwave systems and, hence, cold war optical intelligence is far more difficult than conventional elint. Thus, at present, the Soviet optical warfare capability must be postulated on the basis of tactical need and technical capability.

Because of the inherent line-of-sight restrictions, lack of true sidelobe emissions, and ambient background interference, optical sup-

port measures (OSM) must be specifically targeted and probably provided to the user. This would indicate development of an illumination warning receiver on vehicles.

Soviet tanks are equipped with automatic smoke generators (which provide a form of optical chaff) and, in a manner similar to microwave chaff, optical chaff also can be illuminated by optical sources and thus become a scatterer and jammer. Thus, it appears reasonable to assume that the Soviets will develop a reasonable OW capability.

2-4 (U) MODELS OF THE EW ENVIRONMENT FOR ANALYSIS PURPOSES

2-4.1 (U) GENERAL

The term "model" like the term "vulnerability" has many connotations. Virtually every model is an abstraction designed to analyze a slice of the real world with the object of understanding it better, and if it is at all controllable, adapting it to better serve our needs. Models do not and cannot represent the actual phenomena of reality in all respects. However, they must be carefully designed to represent the inputs, internal characteristics, and outputs to include the diverse, interacting, specialized structure and subdivisions that the model represents. There are three basic types of models: iconic, analog, and symbolic:

a. Iconic Models—models that look like the "thing" being represented. They are usually a small-scale representation of the real. Examples are models of antenna such as a dish, horn, or system mock-up.

b. Analog Models—models produced by a substitution of symbols, lines, etc., to represent the "thing". Examples are a map, a map overlay, a schematic drawing of an electrical circuit. A target array, in particular an electromagnetic target array, is an example of an analog model.

c. Symbolic Models—representations of a "thing" with the use of abstract symbols, for example, a mathematical equation.

Many models of any appreciable size or complexity are compound. A computer simulation is an example of a compound model. Usually, analysis with the aid of a model, in particular, computer simulations, provide analytic, numeric, or Monte Carlo solutions. Solutions of problems by analytic methods frequently use mathematical models in a rather straightforward manner to derive solutions. An example is the solution of jamming equations such as the power-distance equations Solution of problems by numerical methods involves repeated application of the models starting from a set of initial conditions. An example would be the reconstruction of a threat antenna configuration to determine the limit of the radiation pattern. Solutions derived by the use of Monte Carlo methods involve the repeated exercising of the model to determine some probabilistic properties. An example would be Message Analysis simulations to determine susceptibility thresholds, etc. (Refs. 5 and 6).

2-4.2 (U) APPLICATION OF MODELS IN EW

Models, in particular, electromagnetic target* arrays and computer simulation†, are frequently used in EW analysis. Some of the uses of electromagnetic tarays and simulations are: assessment of current and projected threats, evaluation of intercept and jamming tactics, analysis of EW vulnerability, and evaluation of emi.

Mathematical models used in simulation are approximations of real-world phenomena. In

*An em target array, sometime referred to as a taray, is a special application of the TRADOC target array concept.
†See Appendix A for a brief discussion of some of the pertinent simulation packages.

general, validity increases with level of detail and complexity; but a high level of detail does not ensure validity. Regardless of the level of detail, the models should be built on sound engineering and mathematical principles. A fundamental engineering principle is that the errors in the approximations made by the models should be estimated and a level of confidence should be established in the models. This error analysis phase is somewhat difficult in propagation models, and completely lacking in much of the past work. The error analysis is extremely important because analysts tend to treat computer printouts as facts and are likely to make judgments dependent on accuracies not supportable by the accuracy of the models.

A requirement imposed on the structure of the models or programs is that they be efficient in their use of computer time and input data. Flexibility in handling new, unexpected classes of problems is also desirable; this flexibility is achieved through modular structure of the programs. Efficiency in the use of computer time frequently conflicts with the engineering and mathematical validity mentioned previously. If the cost of using the programs is prohibitive, however, the simulation packages are of little value. The use of compact models which minimize the amount of data that must be transferred, the judicious inclusion of detail in the models themselves, and the use of efficient input/output and data-retrieval techniques help to improve efficiency. Efficiency in the use of input data is an important requirement that frequently is overlooked; the cost of preparing input data frequently exceeds the cost of running the simulation. This data-preparation cost leads to the requirement that human engineering go into the preparation of data formats, and that extensive use be made of tables so that input data are not repeated a large number of times.

2-4.3 (U) ELECTROMAGNETIC TARGET ARRAYS (TARAYS)

The electromagnetic taray, an analog model, is a map deployment of radios, radars, intercept gear, jammers, weapon systems, headquarters, control centers, and other things associated with or that have an impact on a battlefield signal environment. These deployments are made in accordance with the doctrine and tactics of the unit or force represented. Deployment configurations are derived from real-world observations or estimates of the projected real world. These deployments usually are made on small scale-maps (1:50,000) (see Fig. 2-7 for a photo of a typical array). Large-scale arrays such as a blue army vs a red army front may have as many as 100,000 individual (x, y) map plots. As a general rule, arrays must be sufficiently detailed to capture the crux of the military situation and yet be sufficiently free of trivial details to achieve a balance between reality and manageability. The quality of the taray data base used in computer-assisted simulations by and large sets the quality level of the simulation.

There are five tasks associated with the development of an array (see Fig. 2-8). These tasks are:

a. Preparation of the electromagnetic model—the development of the CE, EW and EO networks, radiation parameters, and development configurations.

b. Development of the array tactical model—primarily an intelligence research function.

c. Development of the geographic model.

d. Map-plotting function—placing the array elements on the map and the array codification.

e. Recording function—codification of the arrayed data, preparation of the data base cards, and the generation of the deployment file. This task also includes the generation of the emitter and sensor equipment details.

Models of the particular equipment to be analyzed generally fall into two categories: that of transmitters, and that of receivers.

Fig. 2-7 (S). Photo Map of a Target Array Depicting a Warsaw Pact Army Front (U)

These models are essentially a summarization of the technical parameters pertinent to the system analysis. These parameters include frequency, power, antenna-gain characteristics, antenna height, and signal modulation characteristics for transmitters; and frequency, bandwidth, antenna-gain characteristics, antenna height, and sensitivity for receivers. The exact form and level of detail of these models are dependent on the level of detail of the

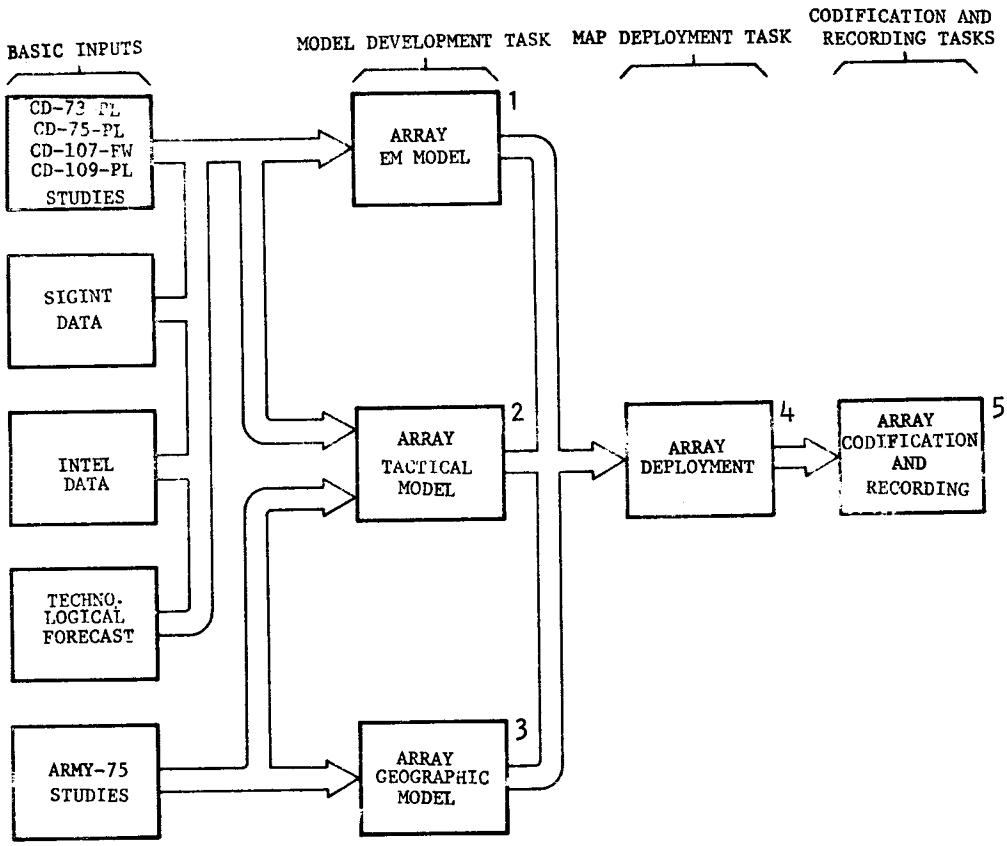


Fig. 2-8 (U). Array Input Flow Chart (U)

overall analysis and the particular means of manipulating data. For instance, the values for the preceding parameters may be assigned to each transmitter or receiver in a deployment model (stored on magnetic tape or punched cards), the median values for the parameters by equipment type may be stored in a look-up table, or the equipment parameters may be assigned in a Monte Carlo fashion, based on the statistics of the parameter ranges. For detailed investigations, functional or analytical models of the equipment occasionally are desired. An electromagnetic array development network diagram is shown in Fig. 2-9.

2-4.4 (U) PROPAGATION MODELS

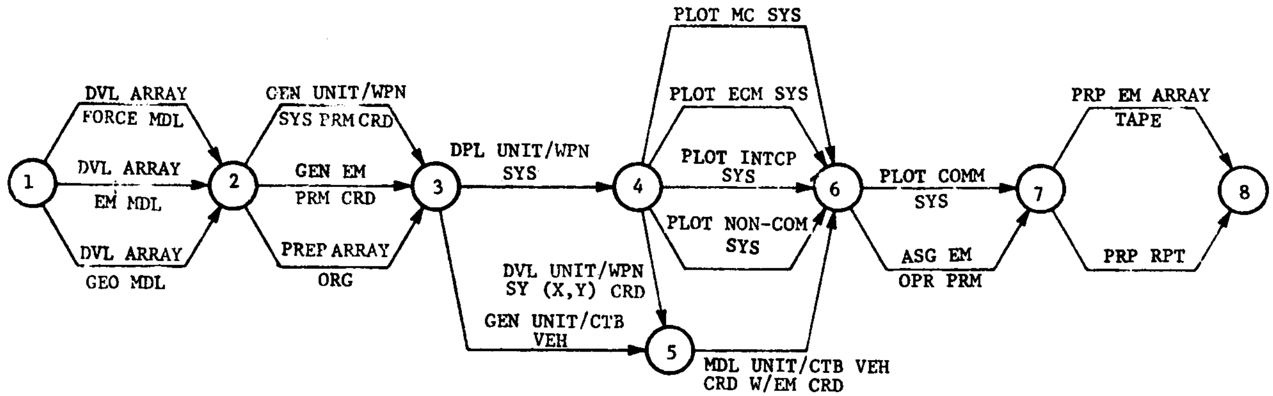
Propagation models generally are subdivided into three major categories according to the frequency band of interest:

a. Medium-frequency (mf) and high-frequency (hf) models

b. Very high-frequency (vhf) and microwave models

c. Optical models.

In each of these categories, different phenomena are significant, thus causing different modeling approaches to be applied. One of the most significant effects on the propagation model structure is that of terrain. In the first category, terrain-profile effects are generally negligible; in the second they have significant effect; and in the third the effect is so great that only path profiles can be employed (line of sight). A brief discussion of the various models is given in the paragraph that follows.



LEGEND:

ASG	ASSIGN	OPR	OPERATING
CBT	COMBAT	ORG	ORGANIZATION
CRD	CARDS	PRM	PARAMETER
DPL	DEPLOY	PRP	PREPARE
DVL	DEVELOP	RPT	REPORT
EM	ELECTROMAGNETIC	SYS	SYSTEM
GEO	GEOGRAPHIC	VEH	VEHICLE
GEN	GENERATE	WPN	WEAPON
MDL	MODEL		

Fig. 2-9 (U). Array Network Diagram (U)

The predominant propagation modes at mf and hf are the ground-wave and sky-wave modes. Propagation effects of these modes can be predicted reasonably well, using analytic techniques. Generally, the same type of analytic approach is taken in most models of this type: they all use sunspot number, time of day, etc., as input data. The primary differences lie in the number of approximations made, and the form and use of the model outputs. These models can be employed on a transmitter/receiver pair basis, or on a generalized numerical map or matrix basis (in view of the independence from the terrain profile). In the first, the frequency, path length, etc., are used in computing propagation loss for each transmitter/receiver pair. In the second, such data are precomputed on a parametric basis such that, for a given path length or frequency, the propagation loss immediately could be found. The latter approach allows for a more detailed analytic technique since large amounts of computer time need not be expended for each transmitter/receiver pair. The errors in the model representation of the propagation phenomena are fewer than the errors encountered by computing the losses for only a small number of time-of-day/time-of-year samples. This results from the great variation in ionospheric characteristics as functions of time of day and time of year.

The predominant propagation modes at vhf and microwave frequencies are line of sight (direct and reflected waves), diffraction, tropospheric scatter, and atmospheric absorption. This is the most difficult frequency region to model since the terrain profile between transmitter and receiver has a significant effect on the propagation loss at these frequencies. All models of any utility have a certain amount of empirical and statistical content. Models have been so designed that the geometry of the discrete path profile is employed directly in the propagation calculations. The propagation calculations themselves, for use with discrete path profiles, may be partially or completely empirical. For instance, the theoretical diffraction and tropospheric-scatter equations may be employed with certain modifications for rough earth based on empirical data, or a model based entirely on experimental results may be employed. In any event, the most widely accepted discrete path profile models developed by NBS/ESSA do not make absolute propagation-loss predictions. Recent comparisons of the median predicted by these models with experimental data in the 400-MHz to 3-GHz region indicate that the error distribution has a bias of 2 dB and a standard deviation of 12 dB. These figures result from averaging over 70 paths, which include line-of-sight and non-line-of-sight geometries. These results are not considered alarming since repeating experiments at different times of the day could well give variations of this magnitude. The important consideration is for the analyst to be aware of the confidence in the estimate in the analysis that follows propagation-loss prediction.

Propagation models also have been designed in this frequency region that employ terrain statistics instead of a discrete path. These models require much less data processing, and attempt to predict the mean and standard deviation of propagation loss in a given type of terrain. Few data are available on the confidence an analyst may have in these loss estimates. Finally, the use of assumed degradation factors, for given terrain classes, may be employed in models wherein the accuracy of results is not critical. These models allow for rapid culling to isolate the paths of interest but are not substantially simpler in their computational requirements than the statistical methods mentioned previously.

The predominant propagation effects at optical frequencies are atmospheric absorption, atmospheric scattering, and atmospheric turbulence. At optical frequencies, terrain obstructions have such a significant effect that terrain information usually is employed only to determine whether optical line of sight exists. Either a statistical or a discrete terrain model can be employed for this func-

tion. The propagation models themselves usually possess a high amount of empirical content. Basically, a decision can be made (based on a discrete or statistical terrain model) as to the existence of optical line of sight. If optical line of sight exists, the geometry of the transmitter/receiver pair is computed and then the propagation effects (absorption, scattering, and turbulence) are determined.

2-4.5 (U) TERRAIN MODELS

As a general rule the incremental detail of the terrain model used in computer-assisted analysis is consistent with the detail of the signal propagation model. For example, if a smooth earth propagation model is used, then an equally coarse terrain model can be used. If, on the other hand, a detailed and precise propagation model is used, then a very detailed model such as the quantification of vegetation, elevation, and soil conductivity data at intervals of 10 km or less is needed. Terrain models range from discrete point-to-point plots to statistically derived Δh models (Δh is a terrain roughness factor).

The discrete terrain models generally contain terrain elevation data (and perhaps foliage data) for each incremental grid point. The path profile then can be determined by finding the terrain elevation points between the transmitter and receiver locations, and interpolating these points to evenly spaced (along the path) elevation points forming the profile.

The statistical terrain models generally are derived from discrete terrain models. Hence, statistical parameters of terrain for given geographical areas are predetermined. Then, either these statistics are employed directly or are input to a stochastic terrain profile generator, which creates profiles based on the statistics of the terrain. This is a more compact terrain model than the discrete point-to-point model. It is, also, much cheaper to develop. The discrete model, however, represents the best approximation of the truth of the real world's geographic form.

(U) REFERENCES

1. JCS Pub 1, *Department of Defense Dictionary of Military and Associated Terms,* the Joint Chiefs of Staff, 3 January 1972.

2. AR 105-2, *Electronic Counter-Countermeasures (ECCM).*

3. AMCR 70-26, *Electronic Warfare Research and Development for Army Missiles,* 18 February 1970.

4. ECOM-5621, *Vulnerability-From an Operational Point of View,* February 1974.

5. *Methodology Notebook for Action Officers,* - (US Army Combat Development Command) (CDC) Now Training and Doctrine Command (TRADOC), May 1967.

6. R. Stone, *Mathematics in the Social Sciences and Other Essays,* MIT Press, March 1966.

7. *ECM Capabilities–EEC* (U), ST-CS-05-18-74, Defense Intelligence Agency, 5 April 1974. (SECRET publication)

8. *ECM Capabilities–Eurasian Communist Countries* (U), Supplement 1: *Ground-Based Electronic Warfare Equipment* (U), Defense Intelligence Agency, 3 May 1974. (SECRET publication)

(U) APPENDIX A

EW-RELATED SIMULATION PACKAGES (U)

(U) This appendix is a survey of some of the simulation packages that can be used in the analysis of EW vulnerability.

A-1 (U) EW SYSTEM ANALYSIS MODELS

A-1.1 (U) ACCESS SYSTEM

ACCESS, an acronym for ASA Computer-Controlled Environmental Simulation System, is a large-scale computer system developed for use with the IBM 7090 or IBM 7094. It provides a system to analyze signal intelligence (sigint), signal security (sigsec), and electronic warfare (EW) missions. The overall ACCESS system is divided into three subsystems, each of which contains a number of specialized computer programs. The first subsystem is used in developing terrain maps, the second is used in constructing the electromagnetic environments that arise from troop deployment, and the third subsystem centers around a high-level computer language designed to facilitate use of the extensive data base provided by the other two subsystems. The way in which each of these three subsystems may be used is described more fully in the paragraphs that follow.

The terrain map subsystem consists of a main program (in FORTRAN IV) and numerous subprograms. The output from this subsystem is a single binary tape that contains terrain data in a format that may be used by the other subsystems. A User Data File (UDF) is a collection of information describing a troop deployment, with particular attention given to the emitters and receivers of the deployment. Normally, one punched card is used to describe a single emitter or receiver. A set of punched cards representing the deployment is used as input by the file maintenance subsystem to make a binary tape. This binary tape itself then is referred to often as the UDF. It is in a format to be used by other subsystems.

The query subsystem is based on a high-level computer language called the Common Intelligence Language (CIL). CIL was designed to be a language that could be grasped quickly by individuals with no previous programming experience, and yet would serve as a language that would allow easy retrieval and processing of data on the UDF and terrain types. Since a CIL program is oriented toward retrieving and processing of items from these extensive data bases, it is called a *query* program. There are eight different types of query statements that may be used, most of which call on modular packages of one or more subroutines for such things as propagation calculation, terrain map interrogation, and data sorting. When a CIL query has been written, it then is translated by the ACCESS query subsystem into a FORTRAN IV program that will contain all the necessary modular subroutines. This FORTRAN IV program (a few of the subprograms will be in assembly language) then can be executed as any other in the batch processing mode. As one would expect, flexibility is limited when programming in CIL, which is an inherent disadvantage of any high-level source language.

The engineering analysis performed by the ACCESS system on data retrieved from UDF's and terrain maps centers around calculation of propagation-path loss. ACCESS has been used for calculating jammer-to-signal ratios, interceptibility, interference, hearability contours, and similar information; but in all of these the

computation of propagation-path loss is fundamental. ACCESS uses six models to predict propagation loss over the range from 0.1 MHz to 40 MHz for path lengths up to 500 km. The Domain I, II, and III models cover the frequency range of 0.1 MHz to 60 MHz via a line-of-sight ground-wave model, a Norton surface-wave (transition shadow region) model, and a Norton surface-wave (far shadow region) model, respectively. The Domain IV model is an ionospheric sky-wave model for the region from 3 MHz to 30 MHz. The Domain V model is a rough-earth model that uses path profiles to predict loss over the 60-MHz to 10,500-MHz range. It considers line-of-sight, single-obstacle, and multiple-obstacle paths. Finally, a microwave model has been added to cover the 10-GHz to 40-GHz region. This model also uses path profiles and considers line-of-sight, diffraction, and tropospheric-scatter propagation paths. All of these models use simple equations that are derived from simplifications of the National Bureau of Standards (NBS) and other theoretical and empirical work. The ACCESS program requires approximately 40 min to make 1,000 path-loss calculations, using an IBM 7094 computer with 12 tape drives.

The principal array using the ACCESS simulation technique is taray alpha. Taray alpha portrays the battlefield signal environment incident to a Central-European mid-intensity conflict situation involving a two-corps blue force field army and a five-army red force army front. The locale is central Europe about 100 km west of the Cheb and Furth Gaps. The array includes headquarters, support, fire, and maneuver air and ground units, and the communication-electronic, sigint, and electronic warfare systems of the red and blue forces.

A-1.2 (U) USAEPG/EMETF MODEL

The Electromagnetic Environmental Test Facility (EMETF) of the US Army Electronic Proving Ground (USAEPG) has a model developed specifically to determine the degree communications and electronics equipments are degraded by both unintentional interference and jamming in a tactical environment.

The model has a library of many modules. An executive routine is used to tailor a model for a specific task. By appropriate tailoring the modeling can provide data on the probability of satisfactory operation of equipments in a specified tactical environment without interference or jamming, with unintentional interference, and with jamming, to include the unintentional degradation caused by the jammer, and the effectiveness of any ECCM techniques employed. The model can be tailored to provide an analysis of both the technical vulnerability of equipments or system and the operational vulnerability of the system in the tactical environment.

Deployment test beds are available from division size to an army in the field complete with Air Force support elements and opposing forces. Deployments vary from current time frame to proposed concepts through 1980.

The model consists of interrelated mathematical models programmed basically in FORTRAN IV for the CDC 6000-Series Computer. The model mathematically simulates the electromagnetic environment of the tactical situation; simulates the CE materiel operating characteristics; and predicts the performance of CE equipments, subsystems, and systems. The mathematical models and the input data are derived from applied theory, supported where possible by empirical data from actual physical measurements.

The model consists of two major sections: the Data Preparation Section and the Interference Prediction Section. There are many separate computer programs and routines within these two sections, which are selected as appropriate for the specific task.

The Data Preparation Section performs two major functions: development and maintenance of a master data base, and extraction

and creation of a task test bed. The master data base is constructed from input data representing the deployment or usage of CE materiel in hypothetical battle actions or scenarios.

The master data base also includes technical data about the CE equipments in the deployment, as well as scoring parameters relating to the satisfactory and unsatisfactory operation of the equipments. The task test bed consists of data selected from the master data base in accordance with the requirements of a specific task.

The Interference Prediction Section consists of a program library and a System Executive. The program library consists of computer programs and routines used in a variety of electromagnetic compatibility evaluations. The System Executive is a computer program that constructs a task or "computational" model by selecting and tailoring appropriate programs and routines from the program library in accordance with the requirements of a specific task. The tailored model consists of only those programs and routines that are necessary to perform the computational phase of the task, including the production of relevant outputs.

The computational model normally consists of four modules: Link Selection, Interference Identification, Scoring, and Output.

The Link Selection module accepts data from the task test bed and selects links to be analyzed in accordance with criteria established in the test plan. The output of the Link Selection module is input to the Interference Identification module. Since the total number of equipments involved in a problem may be very large, a statistical sampling process is used within the Link Selection module to reduce the number of links formed by the CE equipments in the deployment to a practical level for evaluation. The sample size is determined by the level of analytical precision required by the problem. The sampling process is weighted toward selection of those equipments having the greatest relative importance to the accomplishment of the assigned tactical mission.

In the Interference Identification module, the statistics of the desired and interfering signal levels at the input terminals of the receiver of the links being evaluated are calculated. These levels are a function of several factors, including transmitter rf output power, the power gains of the transmitting and receiving antennas, and the basic propagation path loss. The Interference Identification section identifies those transmitters that are potential interferers to each system being evaluated. This determination is based on transmitter power levels, transmitter duty cycles, and receiver characteristics. Duty cycle is defined as the percentage of time a transmitter is actually radiating. The output from the Interference Identification module is input to the Scoring module.

The Scoring module contains programs that compute the probability of satisfactory operation of the equipment being evaluated. The scores are presented in terms appropriate to the particular system being evaluated. The output from the Scoring module is input to the Output module.

The Output module accepts as input the link scores computed by the Scoring module and computes the system effectiveness (SE) of groups of equipments, categorized on the basis of experimental design criteria, in contributing to the success of the assigned military mission. The Output module is also capable of producing low-score analysis of equipments whose scores fall below specified levels. The purpose of these low-score analyses is to provide insight into the probable cause of the low scores. Final outputs from the Output module include both printed and plotted displays of information in camera-ready format.

A-1.3 (U) ALLEN MODELS

The ALLEN Models, written in ALGOL for the Burroughs B-5500 computer, are a set of

programs developed by the ECOM R&D Electromagnetic Environment Division and CEIR, Inc., for the study of electromagnetic compatibility problems. The models include equipment characteristic files, deployment data, propagation loss, receiver-by-receiver interference analysis, and statistical performance summaries. The work is oriented toward electromagnetic compatibility analysis and is similar to that performed at EMETF.

Three major files of data are used for the ALLEN Model. A SITE file is used to describe the *x*-, *y*-, and *z*-coordinates of the equipment; these data are obtained from manual deployments on a map. An EQUIPMENT file describes the equipment characteristics of each type of equipment in considerable detail, including receiver filter characteristics, mixer characteristics, and acceptance ratios. A CIRCUIT file describes the simplex radio communication circuits in terms of transmitter type and identity or location, receiver type and identity or location, receiver priority, and transmitter on-off configuration.

The ALLEN Model includes eight major programs, as depicted in Fig. A-1. The central program is ALLEN "Y", which performs the receiver-by-receiver interference analysis, using statistical propagation/terrain models to determine the six strongest interfering sources. The carrier-to-noise (C/N) and carrier-to-interference (C/I) ratios are then computed at the output of the if and compared with the acceptance ratios. The rf and if selectivity curves, as well as the mixer conversion effects are included in the calculation of if outputs. The system performance then is computed as the probability of receiver failure by integrating the assumed Gaussian density function for the interference.

A-1.4 (U) ELECTRO-OPTICAL MODELS*

The state of development for optical propagation models is not as advanced as that for mf, hf, vhf, and microwave propagation models.

Program BEAM TRAK, an optical model program, calculates the power received from a narrow-band electro-optic source by a receiver located external to the beam. This program, which operates in any three-dimensional transmitter receiver geometry, computes the effects of scattering and absorption by atmospheric constituents. The program was developed for the CDC 3200 computer system.

Program BEAM TRAK calculates the power received in components parallel to the perpendicular to the plane of polarization. The computed power may be either printed or plotted on the CalComp plotter. If the power is printed, each of the two components is given, along with the weighted sum and the average. If the power is plotted, only one of these four powers is given, the choice being up to the user. In any case, the power level is given as a function of angle of observation; the increment on that angle is selected by the user.

During the calculation of the power received, the program computes the volume scattering function for Mie scattering. This function may be printed/plotted as a function of angle of observation, at the option of the user. The amount of scattering and absorption depends upon the aerosol along the path of the beam. The program allows the user to select one of eleven established aerosol modules, including models for haze, cloud, rain, and hail. Each of these models generates a prescribed particle-size distribution. The refractive index of the particles is specified by the user. The user may instruct the program to print the extinction data and the distribution-function value for each particle size considered.

The amount of scattering and absorption depends also upon the temperature and pressure along the beam. The user may specify temperature and pressure data (as a function of altitude) over the altitude range of interest; otherwise, the program assumes the 1962 US Standard Atmosphere. In either case, the temper-

*See also par. 6-2.4.3.1 for examples of electro-optical warfare simulations.

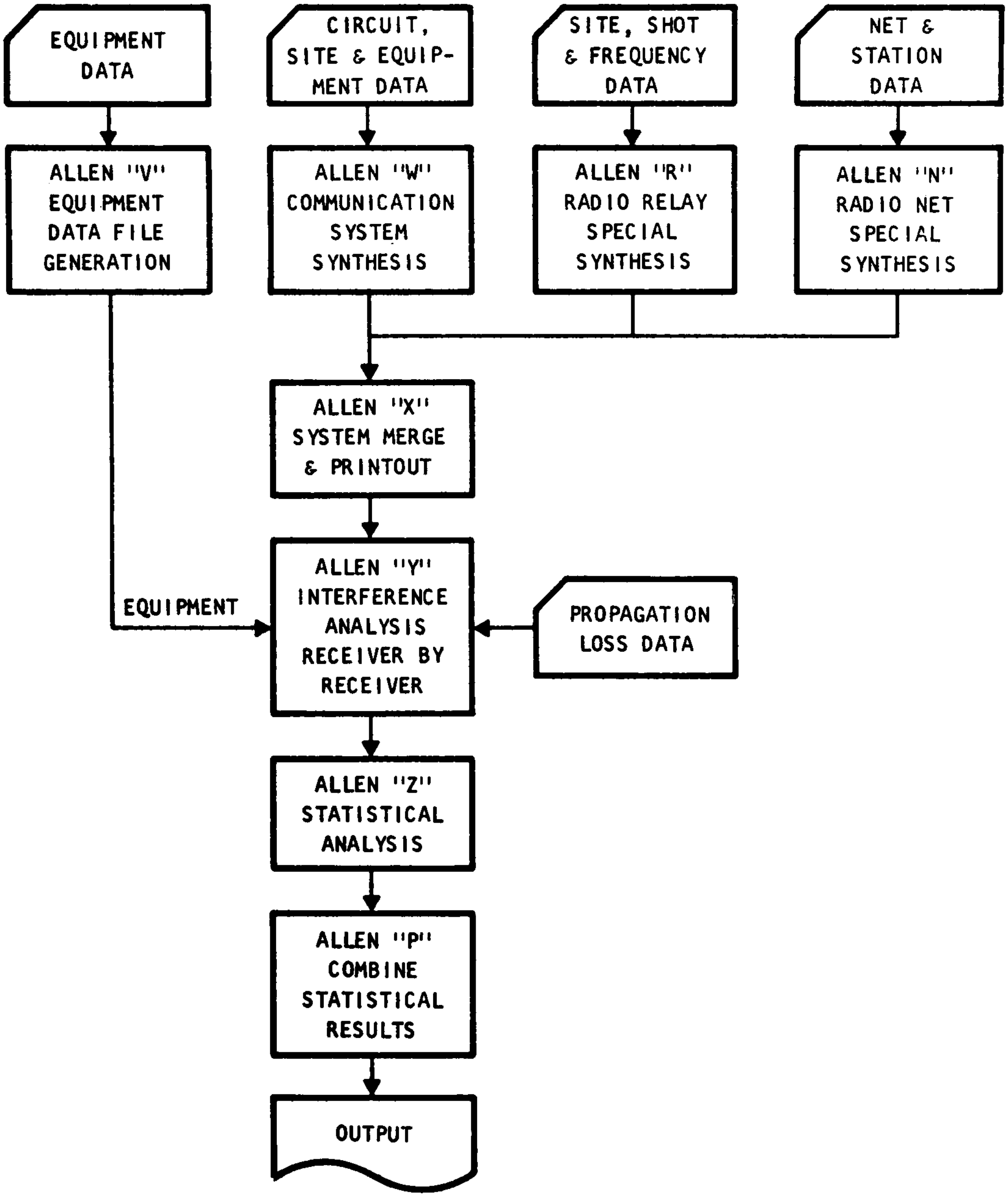


Fig. A-1 (U). The ALLEN Model (U)

ature and pressure data may be printed at the user's option.

The program calculates absorption along the beam by water vapor, carbon dioxide, carbon monoxide, methane, and nitrous oxide. For each gas, the user specifies two wavelength-dependent parameters, along with the mixing ratio of the gas (the amount of gas present) along the beam. If the user fails to specify data for a given gas, the mixing ratio of that gas is assumed to be zero. For each running of the program there is a printed message indicating those gases by which the wavelength under consideration is subject to absorption.

A-2 (U) MESSAGE-ROUTING MODELS

A-2.1 (U) THE HUGHES MALLARD SIMULATION

The Hughes MALLARD I Vulnerability Analysis Simulation program is a large-scale, flexible program that realistically models the complex MALLARD communications network. It uses network and jammer deployments, jammer target assignments, and traffic need-line data in conjunction with message generation to determine traffic and link vulnerability.

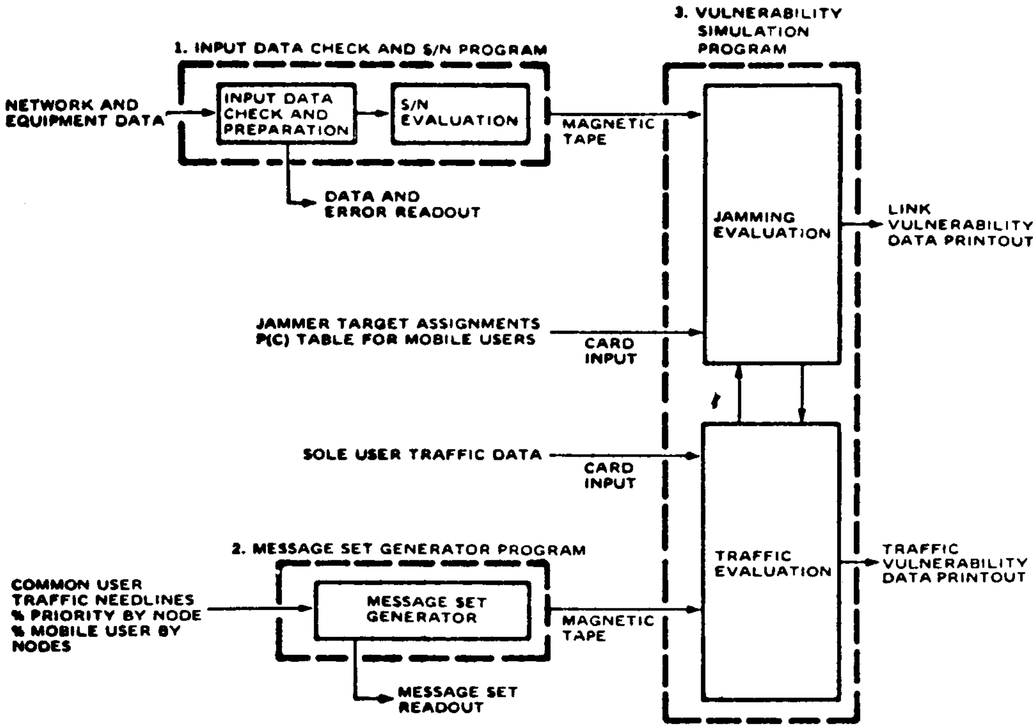
The simulation program consists of three executive programs: (1) the Input Data and Signal-to-Noise program, (2) the Message Set Generator program, and (3) the Vulnerability Simulation program. Each program executes independently, with the first two programs providing input to the third. Fig. A-2 depicts the program structure, and also shows the output data obtainable from the Vulnerability Simulation program.

The Input Data and Signal-to-Noise program sorts and prepares network data, and computes signal-to-noise ratios for input to the third program. The input data consist of the MALLARD I deployment and connectivity information, channel capacities, equipment parameters, and antenna patterns.

A Message Set Generator program generates a common user message set over a full busy hour. Its main functions are to generate and compile statistics on a message set. Three sets of input data are necessary to generate a call. They are the common user need-lines, which specify the amount and type of traffic between node-pairs; the number of preemptive telephone calls by source node; and percent, by node, of the traffic generated by mobile users. The busy hour is represented incrementally by 10,800 time slots, each slot representing 1/3 sec. A call request generated by the computer program is placed with equal probability in one of the time slots between 1 and 10,800. The statistics are computed by source nodes on the number of voice, data A, and fax calls and the number of priority calls generated in time segments of 3-min intervals (540 time slots). A call request generated by the program has five parameters associated with it: time slot of the call request, source node number, sink node number, type of call, and priority. Three types of output are printed: (1) a listing by time slot, at intervals of 540 time slots, of every message, i.e., the five parameters associated with it; (2) a breakdown for every 3 min of traffic by source node of each mode of traffic with totals of priority and nonpriority traffic, with percentages; (3) a breakdown similar to that in (2), but one that shows how much voice traffic at each node was generated by a mobile user at that node.

The jamming and traffic evaluation is performed in the Vulnerability Simulation program. By using input tapes from the Input Data and Signal-to-Noise program and the Message Set Generator program, sole-user traffic, and jammer target assignments, the program attempts to route the generated messages. The simulation operates under the control of a system clock. Each clock time of the simulation represents 1/3 sec of real time. The simulator sets up the sole-user calls (dedicated channels) for the entire time frame and distributes the generation time of the others. Attempts are then made to route all messages generated during the interval. Calls are processed sequentially, with all possible paths (saturation routing) of eight links or less examined. The path of minimum links and maximum S/N is selected. Priority calls are routed over the shortest path, with preemption. Program outputs, providing information on the status of the network in terms of network, traffic, and jammer statistics, are indicated in Fig. A-2.

Statistical signal strength calculations made in the Input Data and Signal-to-Noise program are based on "statistical sidelobe" specification of antenna patterns and one of eight path-loss equations. An antenna pattern is considered



The Three Executive Programs in the MALLARD I Vulnerability Analysis Simulation

OUTPUT DATA OBTAINABLE FROM THE MALLARD VULNERABILITY SIMULATION PROGRAM

- **Jammer effectiveness by types and area**
- **Network traffic loading by links and call types**
- **Traffic statistics by area and call types**
  1. **Number of calls requested**
  2. **Number of successful connections**
  3. **Average number of links per call**
  4. **Number of unsuccessful call requests**
  5. **Calls interrupted by jamming**
  6. **Calls interrupted by pre-emption**
  7. **Completed calls**

Fig. A-2 (U). Hughes Simulation Structure and Output (U)

to have a nonrandom mainlobe and a mean sidelobe level that varies with angle off main beam. A standard deviation about the sidelobe mean value is specified for purposes of a random choice of actual sidelobe gain. In this way the randomness associated with an antenna operating in a field environment is taken into account. The eight propagation equations—handling ground-to-satellite-to-ground, ground-to-ground, air-to-ground, radio relay,

tropospheric scatter, hf groundwave (signals), hf groundwave (jammers), and limiting free space propagation—are based on terrain with vegetated 500-ft rolling hills, as might be found in central Europe. These equations are modifications of the ALLEN model. In the simulation a propagation mode is specified for each link. The mean path loss is calculated from the equation for the particular mode of propagation. A number chosen randomly from a zero-mean normal distribution, with standard deviation appropriate to the chosen propagation mode, is added to the mean path loss. The limiting equation loss is calculated similarly for the same path. The larger loss is selected as the "true" path loss.

A-2.2 (U) IBM ARTSS AND MASS SIMULATIONS

The IBM simulations ARMATS Real-Time System Simulator (ARTSS) and MALLARD Simulating Set (MASS) were designed to address large-scale MALLARD-type communication networks.

ARTSS was developed for use on an IBM 7090 computer and MASS for use on an IBM 360/75 or 360/95 computer. With the exception of capacity, the ARTSS and MASS simulations appear to be similarly oriented in terms of the necessary inputs and the types of answers they were designed to yield, namely, network grade of service, call preemptions, and message path length.

Inputs to ARTSS are network topology and two traffic matrices, one for voice needlines and one for data needlines. Voice calls and data messages are generated from the respective needline matrices, using Poisson arrival rates and mean exponential holding times (different for voice and data). Up to three priorities for both voice and data calls can be simulated. ARTSS contains a complete-path, real-time routing system. The routing scheme is deterministic and uses a shortest-path (in the sense of least "cost") algorithm to determine up to fifteen routes between node pairs. Additionally, up to three routes may be prestored. Voice and data messages are routed end-to-end via routes stored at the initiating node and updated as network status information is processed. The output of an ARTSS simulation run consists of detailed grade-of-service statistics for the overall network, for each originating node, and for each link. It also provides details of call preemption for use in the calculation of continuity of service.

A-2.3 (U) GTE SYLVANIA-SES-EAST AMCN PROGRAM

The Analytical Model of a Communications Network (AMCN) program is written for the medium-sized Control Data Corporation (CDC) 3200 computer, but it could be altered to run on a number of larger machines available at Government installations. Though the AMCN is based on more questionable assumptions (e.g., independence of link blocking probabilities, Poisson-distributed overflow traffic) and is much more restrictive (e.g., no preemptive calls) than ARTSS, grade of service and route-choice results fairly close to those of ARTSS can be obtained with AMCN at a lesser cost of computer time.

The AMCN program avoids direct treatment of propagation, so, like ARTSS, it handles jamming by opening links (probability of blocking increases) or decreasing channel capacity for links equipped for controlled capacity reduction in the face of jamming. The approach to vulnerability analysis, therefore, is based on the specification of rules for selecting those nodes and links within the MALLARD network that are considered to fail as a result of a hostile environment. These rules would be based on the specific character of the threat and the relationship of this threat to a node or link with its specific characteristics. A "threat analysis" group would have to develop such rules and generate "open link" and "reduced capacity" lists before a comparison of grade of service could be made between the jammed and unjammed modes of network operation.

A-3 (U) OTHER MODELS

A-3.1 (U) COMMEL MODEL

The COMMEL model, at Fort Leavenworth, is one of the largest single programs ever writ-

ten for simulation. Unlike many of the models, it originally was designed to be run as a single computer program, not as a series of separate but related programs. The model was intended to be a detailed, realistic, dynamic simulation of combat engagement between two forces of approximately division size; considerable emphasis is placed on simulating the communications in detail. Many features of the tactical action are portrayed in great detail. Tactical movements are a means of generating messages that produce an environment for message flow, and the measuring of the effect of poor communications on combat efficiency. Thus, messages are generated when there is a need for coordination between units, commitment of reserves, direction of artillery fire, or for scores of other reasons. Until the messages get through, the appropriate tactical actions are not taken, resulting in a degradation of the mission effectiveness. The simulation usually covers a period of several hours of combat, during which there will be opportunity for all of the various types of messages to be generated. The computer program originally was designed to be run on an IBM 709 computer, using magnetic tapes for intermediate storage; was later converted to an IBM 7090 computer with disk storage; and is currently being adapted for the CDC 3300 computer.

The simulation model used the COMMEL study at Fort Leavenworth has a long history. Initial work on the model began about 1957 by General Analysis Corporation through a contract issued by the Combat Developments Directorate of the US Army Electronic Proving Ground, Fort Huachuca.

The COMMEL simulator has three large submodels, which interact with each other. These are a tactical submodel, a communications submodel, and a traffic processing submodel. The features of the tactical submodel include movement, fire, and attrition of front-line, reserve, rear-echelon, and artillery units; acquisition and dissemination of intelligence; and command decisions at each of four echelons (usually company, battalion, brigade, and division). The features of a communication system submodel include simulating the communication system itself and the current status of its components. It determines status by evaluating friendly interference, inoperability resulting from enemy action or equipment failures, operability of a link because of unit movement, and similar factors. The traffic processing submodel processes the messages generated by tactical action by computing for each message a delivery time that is a function of message length, encoding or encrypting time, queue delays, interference delays, switching delays, and decoding or decrypting time. These submodels interact during a simulation. As the simulation progresses, important actions of the combat elements such as commitment of reserves, coordination of fires, selection of targets, effects of artillery, and movement of units are dependent upon the generation and delivery of messages associated with these events. Thus, a poor communication system will result in message delays and failures that significantly degrade combat power from what it would be with a better system.

A-3.2 (U) CRESS

The Combined Reconnaissance, Surveillance, and Sigint (CRESS) model is a man/computer model designed by Stanford Research Institute to simulate the operational use and data outputs of reconnaissance and surveillance (R&S) systems built around collections of sensors. The simulation of the operational use of any collection of sensors of these types produces: (1) the target element detection capability, (2) the location and location accuracy, and (3) the timeliness of generated reports, as the basic measures of performance of the systems.

A large-scale (65,000 words of core storage), high-speed digital computer with a random-access disk, and persons knowledgeable in scenario development, sensor deployment, and intelligence analysis are required to exercise CRESS. CRESS uses the computer for all mathematical calculations, most of the bookkeeping and printing of sensor system performance, and men for deployment of the sensors (both sigint and non-sigint), data manipulation, and analyses of the resulting data.

(C) CHAPTER 3

EW VULNERABILITY OF TACTICAL COMMUNICATIONS (U)

LIST OF ABBREVIATIONS

ABBREVIATION	DEFINITION
ACSI	Assistant Chief of Staff for Intelligence (Headquarters, Department of the Army)
afc	automatic frequency control
agc	automatic gain control
AI	articulation index
alc	automatic load control
am	amplitude modulation
ber	bit error rate
bpsk	biphase shift keying
bw	bandwidth
C/N	carrier-to-noise ratio
$(C/N)_i$	carrier-to-noise ratio at receiver input (ratio of average of total signal power in receiver if to average of total noise power in receiver if for bandwidth $\dot{B}_{IF}$)
CCIR	Comite Consultatif International Radio (International Radio Consultative Committee)
cm	centimeter
cw	continuous wave
dB	decibel
dBm	decibels referenced to 1 mW
dBW	decibels referenced to 1 W
deg	degree
df	duty factor
dsb	double sideband
ECCM	electronic counter-countermeasures
ECM	electronic countermeasures
ECOM	(US Army) Electronics Command (USAECOM)
EDL	Electronic Defense Laboratories (GTE Sylvania)
ESM	electronic warfare support measures
ESSA	Environmental Science Services Administration
EW	electronic warfare
fdm	frequency division multiplex
FIO	Foreign Intelligence Office

ABBRE-VIATION	DEFINITION
fm	frequency modulation
fsk	frequency shift keying
FSTC	(Army) Foreign Science and Technology Center
GHz	gigahertz
GTE	General Telephone and Electronics
hf	high frequency (3-30 MHz)
Hz	hertz
icd	imitative communication deception
if	intermediate frequency
isnr	instantaneous signal-to-noise ratio
J	joule
JASA	Journal of the Acoustical Society of America
J/S	jamming-to-signal ratio
$(J/S)_A$	J/S ratio actually present at a receiver input
$(J/S)_R$	J/S ratio required to jam
J/Sp	J/S ratio with signal peak envelope power being measured
$(J + N)/S$	jamming plus noise-to-signal ratio
kHz	kilohertz
lf	low frequency (30-300 kHz)

ABBRE-VIATION	DEFINITION
mf	medium frequency (300-3000 kHz)
MHz	megahertz
MIL/POL	military/political
msec	millisecond
pam	pulse amplitude modulation
pb	phonetically balanced
pcm	pulse code modulation
pdf	probability density function
pll	phase-locked loop
pm	phase modulation
ppm	pulse position modulation
pps	pulses per second
prt	pulse repetition frequency
psk	phase shift keying
pw	pulsewidth
qpsk	quadriphase shift keying
S/I	signal-to-interference ratio
S/N	signal-to-noise ratio
$(S/N)_I$	S/N ratio required at an intercept receiver
$(S/N)_o$	S/N ratio at the receiver output
$(S + N)/N$	signal plus noise-to-noise ratio
sec	second

ABBRE-VIATION	DEFINITION
sigint	signal intelligence
SRI	Stanford Research Institute
ssb	single sideband
ssbsc	single-sideband suppressed carrier
T/T_o	relative message delay
TT/N	test tone-to-noise ratio
tdm	time devision multiplex
vhf	very high frequency (30-300 MHz)
vlf	very low frequency (3-30 kHz)
wpm	words per minute
xmt	transmit
xmtr	transmitter

LIST OF SYMBOLS

A	physical area of antenna aperture, m^2
A_r	effective antenna area, m^2
B	receiver rf bandwidth, Hz
B	intercept receiver noise bandwidth, Hz
B_a	audio bandwidth (of an audio signal), Hz
B_A	audio bandwidth of target receiver, Hz

ABBRE-VIATION	DEFINITION
B_J	bandwidth of modulating jamming signal, Hz
B_n	noise bandwidth (of a noise signal), Hz
B_{NOISE}	bandwidth of modulating noise, Hz
B_R	rf/if bandwidth of target receiver, Hz
B_S	bandwidth of modulating signal, Hz
d	path distance, m
D	antenna aperture diameter, m
D	antenna directivity; ratio of max antenna radiation intensity to average radiation intensity, ratio or dB
d_I	path distance between transmitter and intercept (ESM) receiver, m
d_J	path distance between jammer and target receiver, m or km
D_J	frequency deviation of jamming signal, Hz
d_S	signal path distance (between transmitter and receiver), m or km
D_S	frequency deviation of target signal, Hz
E	energy in one bit, J
$erf(x)$	error function, dimensionless

$erfc\ (x)$	complementary error function, dimensionless
f	frequency, Hz
f_J	frequency of jamming signal, Hz
f_{max}	highest frequency component in the baseband, Hz
f_R	frequency to which target receiver is tuned, Hz
f_S	frequency of target signal, Hz
G	*See:* $G\ (\theta, \phi)$.
G_I	intercept (ESM) receiver antenna gain, ratio or dB
G_J	jammer antenna gain, ratio or dB
G_R	receiving antenna gain, ratio or dB
G_{RJ}	target receiver antenna gain in direction of the jammer, ratio or dB
G_T	transmitting antenna gain, ratio or dB
G_{TI}	transmitting antenna gain in direction of intercept receiver, ratio or dB
G_θ	gain of an antenna whose plane of linear polarization is different from that of the incident field by an angle θ, ratio or dB
$G\ (\theta, \phi); G$	antenna gain function; antenna gain as a function of direction defined by angles θ and ϕ in a polar coordinate reference system, ratio or dB
$h_{e_{min}}$	minimum effective antenna height, a limiting value governed by frequency, soil conductivity, and dielectric constant, m
h_I	intercept antenna height, m
h_{Ie}	effective intercept antenna height, m
h_{Je}	effective jammer antenna height, m
h_R	physical height of receiving antenna, m
h_{Re}	effective receiving antenna height, m
h_T	physical height of transmitting antenna, m
h_{Te}	effective transmitting antenna height, m
$H1$	transmit antenna height, m
$H2$	receive antenna height, m
$\hat{I}$	peak interference power, W
J	average power of jamming signal, W or dBW
J_c	carrier power of jamming signal, W or dBW
J_p	peak jamming power, W or dBW
k	Boltzmann's constant, 1.38×10^{-23} J • °K^{-1}
k	antenna efficiency factor, G/D, dimensionless
k	number of symbols in a data sequence of an M-ary signaling scheme, dimensionless

L	physical length of antenna, m
L_I	mean propagation loss between transmitter and intercept receiver, dB
L_J	mean propagation loss over the jamming path, dB
L_S	mean propagation loss over the signal path, dB
M	number of signals available at transmitter for an M-ary digital signaling scheme, dimensionless
M	vocabulary size, dimensionless
m_J	effective or rms modulation index of jamming, dimensionless
m_S	effective or rms modulation index of signal, dimensionless
N	noise power, W
N	mean value of a normally distributed random variable, (various)
N_0	noise power density, J or $W \cdot Hz^{-1}$
P	power density, $W \cdot m^{-2}$
P_B	probability of bit error, dimensionless
P_E	probability of sequence error ($P_B = P_E$ for a binary digital system), dimensionless
P_e	probability of bit error, dimensionless
P_J	output power of jammer transmitter, W or dBW
P_T	transmitter power, W or dBW
R	maximum radio line-of-sight distance between transmitter and receiver (4/3 Earth), m
R	decay rate of automatic load control (alc), $dB \cdot sec^{-1}$
R	data transmission rate, bits per sec
S	average power of target signal, W or dBW
S	signal power, W
S_c	carrier power of target signal, W or dBW
S_p	peak envelope power of target signal, W or dBW
$s_j(t)$	one of the signals available at the transmitter for transmitting the M possible signals, V
T	bit duration, sec
T	duration of $s_j(t)$, sec
T_I	total intercept system noise temperature, °K
TB	receiver processing gain, $sec \cdot Hz$
W_J	bandwidth of jamming signal, Hz
W_S	bandwidth of target signal, Hz
β	fm deviation ratio, dimensionless
Δf, Δf_S	carrier offset (offset between jamming and signal carriers), Hz

ϵ	soil relative dielectric constant, dimensionless
η	mean value of gain in antenna sidelobe structure, dimensionless
θ	angle between radio horizon rays in the great circle plane (troposcatter propagation), rad (or deg)
θ_E	antenna beamwidth in the E-plane between half-power points, deg
θ_H	antenna beamwidth in the H-plane between half-power points, deg
λ	wavelength, m
π_j	prior probability of $s_j(t)$, dimensionless
ρ	correlation coefficient, $-1 \leqslant \rho \leqslant 1$, dimensionless
σ	soil conductivity, mhos/m
σ^2	variance of the distribution of a random variable, various
$\phi(t)$	phase error in phase-locked loop, rad (or deg)

3-1 (U) INTRODUCTION

3-1.1 (U) SCOPE

This chapter presents a methodology for calculating the EW vulnerability of tactical communication equipment. It concentrates on the vulnerability of a single radio set, because this is the basic calculation required to establish the vulnerability both of a communications link and of a network of many communication links.

Chapter 3 is addressed in particular to engineers who are involved in the design of communication equipment but who do not have extensive experience in EW analysis. Such engineers employed by the Government or under contract to the Government may, in the course of designing or evaluating communication equipment, find it necessary to determine the vulnerability of the equipment to EW; i.e., to jamming or to intercept. This chapter is meant to provide them with sufficient information to carry out a straightforward vulnerability analysis of the equipment. Analyses of the vulnerability of communication networks and trunk communications are usually much more complex than the analysis of the vulnerability of a single equipment; however, these more complex analyses may be organized or developed following the procedures used in the more simple analyses presented here.

The communication equipment under consideration is limited to tactical equipment such as that used by US Army units. It includes single-channel hf-am, hf-ssb, and vhf-fm used for voice and teletype; and multichannel trunk equipment such as uhf and microwave ssb/fdm/fm and pcm/tdm/fm.

3-1.2 (U) OUTLINE OF THE METHODOLOGY

Vulnerability of communication equipment to electronic warfare is determined by four factors: susceptibility, accessibility, interceptibility, and feasibility. These terms are defined in Chapter 2.

Susceptibility, applied to communications, often is expressed as a plot of communications performance vs jamming-to-signal ratio (jsr), which is expressed symbolically as J/S. A single piece of communication equipment will have many different susceptibility curves, because each different kind of jamming signal results in a different curve (as do changes in parameter values of the receiver and the target signal).

Interceptibility is determined by comparing the signal-to-noise ratio (snr) required at an intercept receiver, $(S/N)_I$, for detection, direction finding, or other parametric estimation with the actual snr, S/N, of the received signal. If $S/N \geqslant (S/N)_I$, the signal is interceptible.

Accessibility is determined by calculating the actual jsr, $(J/S)_A$, present at a receiver input and comparing it with the jsr required to jam, $(J/S)_R$. If $(J/S)_A \geqslant (J/S)_R$, the receiver is accessible.

Feasibility is determined subjectively. If the threat, i.e., the hostile EW capability necessary for accessibility or interceptibility is concluded to be infeasible on technical, military, or economic grounds, or if it is concluded that a hostile force would not carry out EW even if it were capable of it, then a communication system is not vulnerable to the threat even if it is accessible to and interceptible by the threat.

The steps an engineer must follow to determine EW vulnerability of a communication equipment are:

(1) Establish the threat, i.e., the EW capabilities of the potential adversary. This includes characteristics, actual or postulated, of his EW equipment or a prediction of what he may develop at a future time. It also includes information about how he will deploy and use the equipment or an evaluation of his capability to develop the needed technology by a specific time.

(2) Describe the target equipment. This is the "friendly" equipment whose EW vulnerability the engineer is analyzing. This step includes determining all the pertinent technical information about the equipment and a description of how and where the equipment is to be used in practice.

(3) Establish susceptibility. This step may be done analytically, experimentally, or both. Susceptibility curves may have been generated already or the engineer may have to generate them himself. A curve must be generated for each kind of jamming signal the adversary is likely to use.

(4) Establish interceptibility. The target signal that may be jammed must be intercepted before it can be jammed. This is necessary in order to measure frequency and other parameters that must be known to generate an effective jamming signal and, in addition, to know when the target signal is on the air so as to know when to jam. Intercept is sometimes necessary to locate the target receiver by obtaining a fix on the collocated transmitter.

(5) Determine accessibility. This usually is done analytically. Results may be corroborated experimentally. The engineer calculates propagation loss, antenna gains, and other effects that occur between potential jamming transmitter locations and the target receiver to determine if the jamming signal will arrive at the receiver with sufficient strength to jam it.

(6) Determine feasibility. If the target communication terminal is accessible and interceptible, then the engineer investigates feasibility. From information gathered about the threat he evaluates whether the potential adversary is able to field the postulated threat or if there are considerations that would have him choose not to carry out EW even if it were possible to do so.

(7) Determine communication network/trunk communication vulnerability. If individual communication links are vulnerable, the engineer may want to determine the effect on the survivability of a net or trunk. Here he must take into account alternate routes, alternate frequencies, network topology (how many nodes of the net must be jammed to prevent high priority communications).

An elaboration of these steps is the subject of the remainder of Chapter 3.

3-2 (U) ECM SUSCEPTIBILITY LEVELS

3-2.1 (U) SUSCEPTIBILITY

Susceptibility is defined in par. 2-2.2 of Chapter 2. It relates, quantitatively, the jamming at the receiver input to receiver performance. A common way to express susceptibility is by a curve of receiver performance vs *J/S*. For example, susceptibility may be expressed in terms of a *J/S* curve (the ratio of jamming power to signal power) at the input of a digital receiver vs bit error rate at the receiver output. A point on this curve of particular interest is the "susceptibility threshold" point, i.e., the point at which the jammed condition is considered to begin. In the hypothetical susceptibility curve of Fig. 3-1, if a bit error rate (ber) of 10^{-1} is taken to be the jammed condition, then the susceptibility threshold is a jsr of 8 dB.

Fig. 3-1, if it represented the susceptibility of an actual receiver, would apply only for one fixed set of conditions on the receiver, on the target signal, and on the jamming signal, as will be discussed. Moreover, the curve undoubtedly would have been generated in a laboratory under fairly ideal conditions. Therefore, the numerator of the *J/S* ratio represents nearly pure jamming power. However, in the field the same receiver would have to operate in a noise environment. Therefore, a jamming signal would add to the already present noise. If the signal power is already close to the noise power, the jsr required to jam in the field is to be lower than the *J/S* ratio required to jam in the laboratory. However, if $S \gg N$ in the field, then the laboratory and field jsr

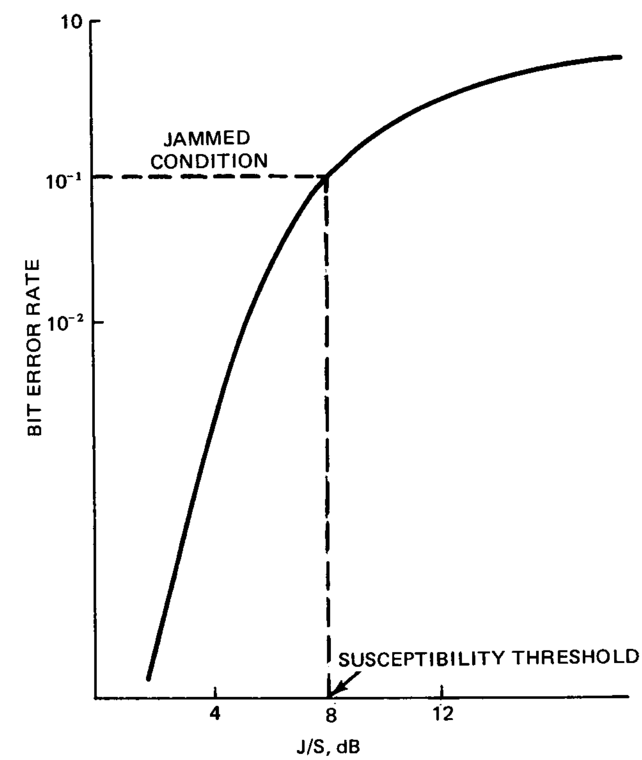


Figure 3-1 (U). A Theoretical Susceptibility Curve for Purposes of Illustration (U)

will not differ measurably. Finally, the bit error rate at the receiver output that is considered the jammed condition is one that is selected subjectively. It is not an arbitrary choice, but it is a choice. Usually it is based on a consensus of users on the point at which performance has become so degraded that the service is no longer usable or the accuracy of the information is undependable.

3-2.1.1 (U) Conditions That Must Be Specified When Expressing Susceptibility

A susceptibility curve is valid only for the conditions under which it was generated. For example, the curve, in general, would not be valid for a different jamming signal, e.g., fm-by-wideband noise in place of rf noise. As shown in Fig. 3-2, these two jamming signals result in two separate susceptibility curves, even if all other parameter values are held constant. A large number of parameters affect susceptibility and should be of a fixed, known value when generating a susceptibility curve. The important parameters–associated either with the target signal, the jamming signal, or the target receiver–are listed in Table 3-1. Note that in order to use Fig. 3-2, values of these parameters would have to be specified. This is necessary to ensure that these susceptibility curves are not used for conditions they do not represent.

3-2.1.2 (U) Receiver Performance and Selection of Susceptibility Threshold in Terms of Performance

Susceptibility curves are plots of receiver performance vs jsr. Receiver performance can be expressed quantitatively in several ways. Some of the common measures of receiver performance are:

(1) Bit error rate (ber) or probability of bit error (expressed by the term P_e)

(2) Character error rate

(3) Signal-to-noise ratio (expressed as S/N) or variants such as signal-to-interference ratio S/I or test tone-to-noise ratio TT/N

(4) Intelligibility

(5) Map time

(6) Relative message delay.

These measures are discussed in the paragraphs that follow.

3-2.1.2.1 (U) Bit Error Rate (BER)

Bit error rate or probability of bit error is a useful way to express performance of a receiver if the output of the demodulator is a certain kind of binary digital stream of pulses such as pcm. (It is not useful for every kind of digital receiver; for example, it is not a good measure of performance in ppm, pdm, or pam receivers.) Bit error rate in a pcm bitstream, for example, can be used as a performance measure regardless of whether the bitstream is converted later to analog, as in digitized voice; converted to another form of digital coding; or used as is. However, once a susceptibility curve of ber vs J/S is generated, the selection of the ber that is taken to be the threshold or jamming depends on the final receiver output. For example, if a pcm bitstream is converted ultimately to a voice output, then the ber in the pcm bitstream that corresponds to jammed speech at the receiver output should be selected as the threshold performance beyond which the voice output is no longer intelligible. This threshold ber will be different for different kinds of receivers. For example, the performance of pcm voice systems has been found to be sensitive to the kind of sync circuit that is used. Pcm voice is usually intelligible except when the receiver is not in sync. Two different receivers may lose sync at different ber's; one may be able to regain sync in the presence of a

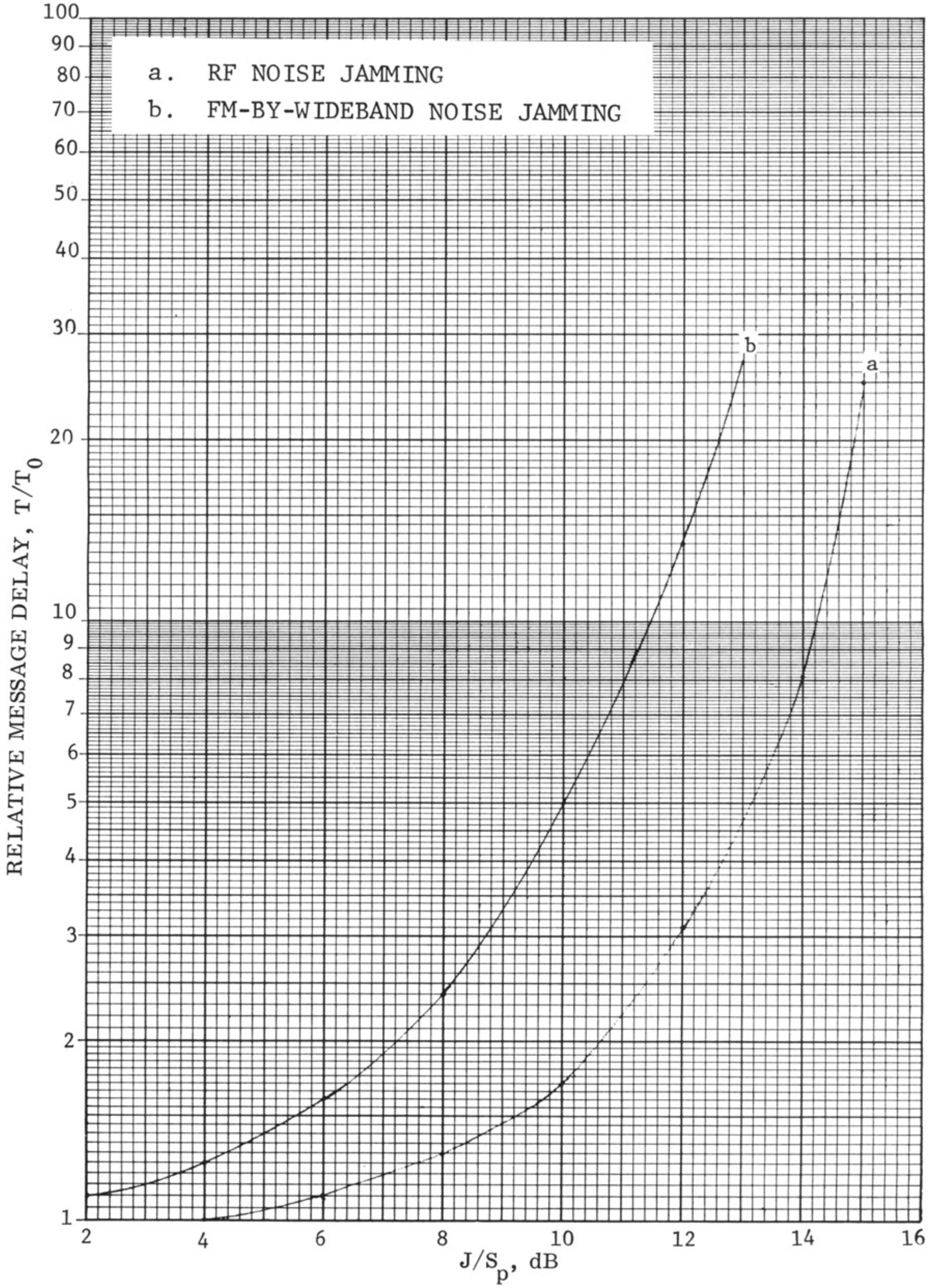


Figure 3-2 (U). Susceptibility Curves Showing the Effect of Changing One Parameter (U)

TABLE 3-1 (U). SIGNAL AND RECEIVER PARAMETERS (U)

A. TARGET SIGNAL		
	S	= Average power of target signal
	S_c	= Carrier power of target signal
	S_p	= Peak envelope power of target signal
	f_S	= Frequency of target signal
	B_S	= Bandwidth of modulating signal
	m_S	= Effective or rms modulation index
	W_S	= Bandwidth of target signal
	D_S	= Frequency deviation of target signal
B. JAMMING SIGNAL		
	J	= Average power of jamming signal
	J_c	= Carrier power of jamming signal
	f_J	= Frequency of jamming signal
	B_J	= Bandwidth of modulating signal
	m_J	= Effective or rms modulation index
	W_J	= Bandwidth of jamming signal
	D_J	= Frequency deviation of jamming signal
C. TARGET RECEIVER		
	f_R	= Frequency to which target receiver is tuned
	B_R	= Rf/if bandwidth of target receiver
	B_A	= Audio bandwidth of target receiver

higher ber than the other receiver can. Therefore, if the ber of 10^{-1}, for example, is the threshold for a pcm voice communications system, the threshold might be 2×10^{-1} for the identical signal and identical jamming in a receiver that is different beyond the demodulator. Note that, in this case, even the susceptibility curves could be identical. However, the jamming thresholds on the curve are different.

3-2.1.2.2 (U) Intelligibility Testing

Intelligibility testing is an obvious way to evaluate the performance of a communication system designed to transmit the human voice intelligibly. Intelligibility can be measured by the percentage of correctly received monosyllabic nonsense words uttered in an uncorrelated sequence. This score is known as syllable articulation. Because the sounds are nonsense syllables, one part of the word is entirely uncorrelated with the remainder; so it is not possible consistently to guess the whole word correctly if only part of it is received intelligibly. Obviously, if the test speech were a commonly used word, or say a whole sentence with commonly used word sequences, the score would increase because of correct guessing from the context. Fig. 3-3 shows the interrelationship between syllable, word, and sentence articulation. Also given is a quantity known as articulation index (Ref. 1).

The concept and use of articulation index is obtained from Fig. 3-4. The abscissa is divided into 20 bandwidths of unequal frequency interval. Each of these bands will contribute 5 percent to the articulation index when the speech spectrum is not masked by noise and is sufficiently loud to be above the threshold of audibility. The ordinates give the root-mean-square peaks and minimums (in 1/8-sec intervals), and the average sound pressures created at 1 m from a speaker's mouth in an anechoic (echo-free) chamber. The units are in decibels pressure per hertz relative to a pressure of 0.0002 dyn/cm^2. [For example, for a bandwidth of 100 Hz, rather than 1 Hz, the pressure would be that indicated plus 20 dB; the latter figure is obtained by taking 10 times the logarithm (to the base 10) of the ratio of the 100-Hz band to the indicated band of 1 Hz (Ref. 1).]

An articulation index of 5 percent results in any of the 20 bands when a full 30-dB range of speech-pressure peaks to speech-pressure minimums is obtained in that band. If the speech minimums are masked by noise of a higher pressure, the contribution to articulation is reduced accordingly to a value given by [1/6] [(decibel level of speech peaks) - (decibel level of average noise)], percent. Thus, if the average noise is 30 dB under the speech peaks, this expression gives 5 percent. If the noise is only 10 dB below the speech peaks, the contribution to articulation index reduces to 10/6 percent = 1.67 percent. If the noise is more than 30 dB below the speech peaks, a value of 5 percent is used for the articulation index. Such a computation is made for each of the 20 bands of Fig. 3-4, and the results are added to give the expected articulation index (Ref. 1).

In recent years a number of automatic speech intelligibility devices have been proposed (for example, Refs. 3 and 4). Most of these devices make the appropriate measurements and calculations described previously to determine the articulation index. A number of important results follow from Fig. 3-4. For example, in the presence of a large white (thermal-agitational) noise having a flat spectrum, an improvement in articulation results if preemphasis is used. A preemphasis rate of about 8 dB/octave is sufficient.

There are several different intelligibility tests in use, characterized primarily by the different word lists used in each test. The objectives of each test vary, but in general they seek to evaluate the performance of a voice communication system quantitatively in a way that is repeatable and that can be correlated directly with the performance of the system when it is in practical use under the same conditions of interference that are imposed by the test. Some difficulty arises when attempting to compare two systems that have been evaluated by different intelligibility tests. However, a number of investigations have been carried out to establish the relationships among results of the most common intelligibility tests. In the past, many

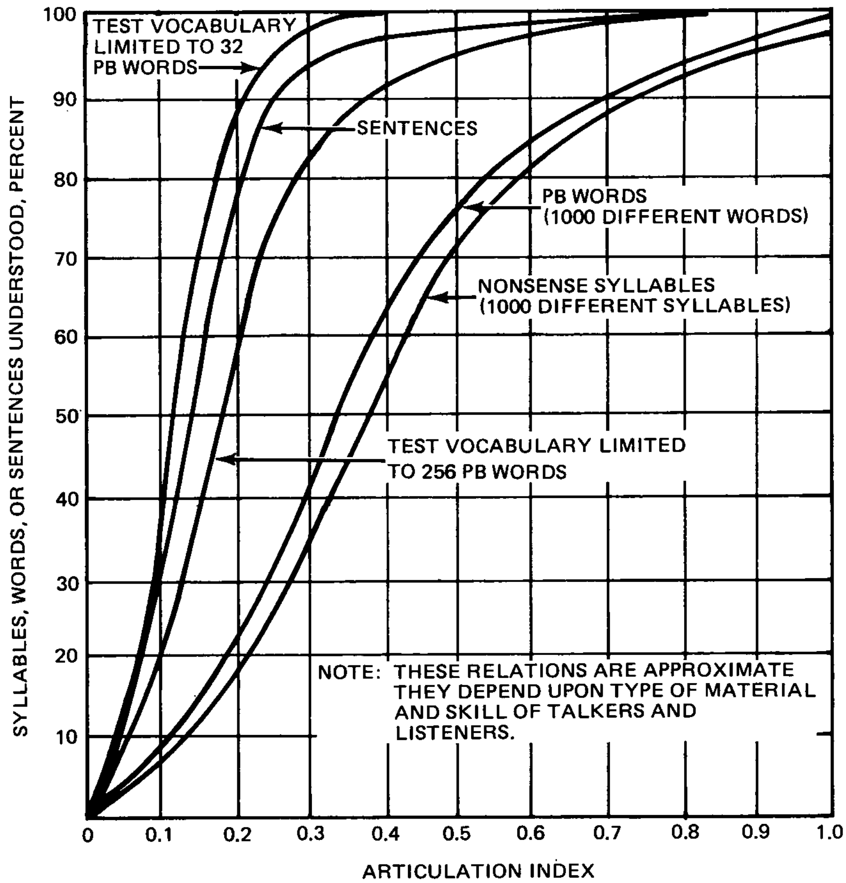


Figure 3-3 (U). Relation Between AI and Various Measures of Speech Intelligibility (Ref. 2) (U)

speech-communication systems have been measured with the Harvard phonetically balanced* (PB) word tests (Ref. 5). Fairbanks (Ref. 6) constructed a different type of word test, which he named the "rhyme" test, that is suitable for measuring the performance of speech-communication systems. More recently, a so-called "modified rhyme" test (Ref. 7) has been developed for speech-system evaluation, particularly when the systems are being tested under operational or "field" conditions. A test related to the Rhyme Test and the Modified Rhyme Test is called the Rhyming Minimal Contrast Test (Ref. 8). Other tests are the Consonant-Nucleus-Consonant List Test (Ref. 9), the Consonantal Differentiation Test (Ref. 7), and the Spondee Word List Test (Ref. 10).

The relationship among several of these intelligibility tests has been investigated by Kryter and Whitman (Ref. 11) and is shown in Fig. 3-5.

There are many facets of language and test design that must be understood, controlled, and specified before any quantitative score has any meaning. A user must understand which test is appropriate for his needs.

*That is, the phonemic statistics of the lists reflect the overall phonemic structure of the English language.

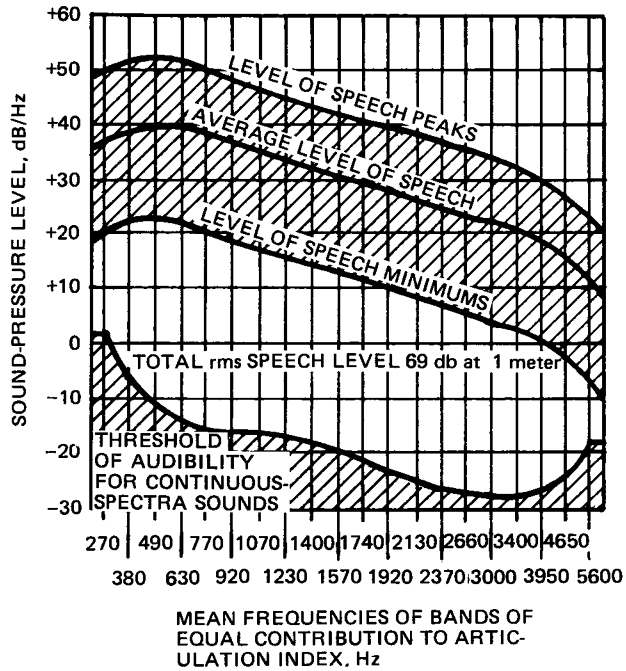


Figure 3-4 (U). Bands of Equal Articulation Index (U)

Preference of a particular test generally depends on the effort required to administer and score the test, and on the importance of various language factors in a specific application. Early phonetically balanced word list tests required several weeks of training and were difficult to interpret and score. Recently developed tests such as the Krual and House Modified Rhyme Test are easy to administer and require only about 90 sec (Ref. 12) to complete a 50-word test segment. Also, tests consisting of spoken digits (Ref. 13) instead of words require no vocabulary familiarization time and are administered easily. Language factors considered important variables in intelligibility testing include vocabulary size (number of words of digits), vocabulary type (PB, Rhyme, Sentence, Digits), word familiarity (frequency of occurrence in a language), response alternatives (size of multiple choices), phonetic elements (consonant and vowel test dependencies), and context (sentence or message).

Additional factors relating to colloquialisms, military or civilian speech, and test presentation format also must be considered to ensure that a "realistic" test is conducted. Since elements such as speaker voice characteristics, speaking rate, enunciation, context, and volume are important perception clues to the listener, a carrier phrase presentation format frequently is used in word or digit testing. This allows the listener's ear-brain perception process to tune in to the desired signal by discriminating against various types of interfering sounds. Test results may vary up to 6 dB in terms of signal-to-interfering-signal ratio, depending on whether a carrier phrase format is used or if a word merely is

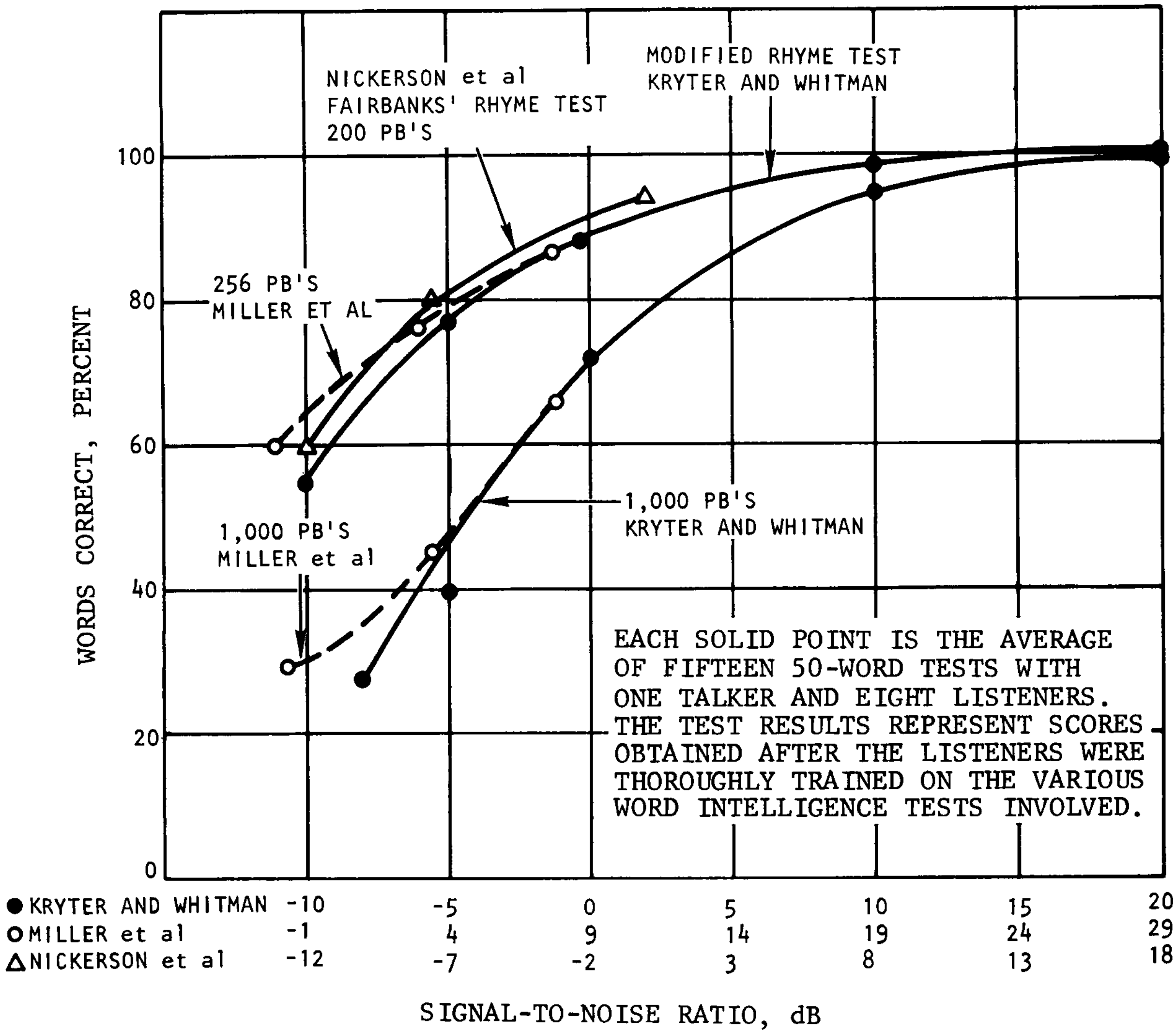


Figure 3-5 (U). Relationship Between Percentage of Words Correct and SNR (U)

repeated by itself. The carrier phrase format allows the listener to sensitize and anticipate the volume and time of occurrence of the test word and thus more closely represents the conditions of a message lasting several seconds. Further, this format requires more interference power than the single-word format and thus leads to more conservative estimates in assessing receiver vulnerability to interference.

It should be noted that equipment factors are also of key importance in evaluating communication system performance. Audio processing such as preemphasis and peak clipping can greatly increase speech intelligibility in the presence of interference. Such processing increases the relative strength of consonant and other weak sounds. Since the majority of rhyme tests measure confusion among consonants (consonants being much weaker than vowels in unprocessed speech), speech processing can impact strongly on such test results and less strongly on tests designed around balanced consonant/vowel factors. Careful considera-

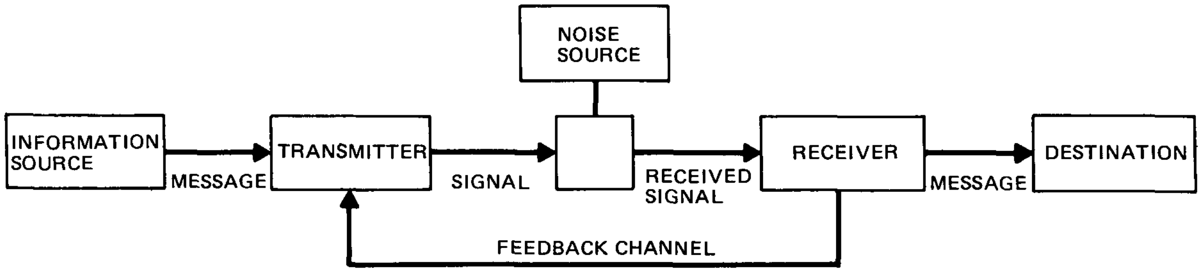


Figure 3-6 (U). Basic Communications System (U)

tion must also be given to the differences in radio frequency processing of receiver systems. The well known "capture effect" of fm receivers requires only a few decibels difference in radio frequency power to produce a large change in audio intelligibility. Also, a small change in am modulation index will cause a large change in am receiver audio intelligibility. Therefore, it can be seen from the preceding discussion that intelligibility testing involves awareness and control of numerous variables relating to testing material and procedures, as well as language and equipment factors, to obtain valid test results.

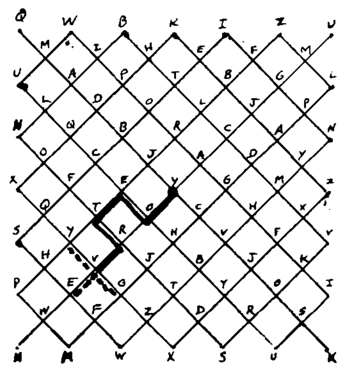


Figure 3-7 (U). The Michigan Diamond Map No. 4 for Six-Town Routes (U)

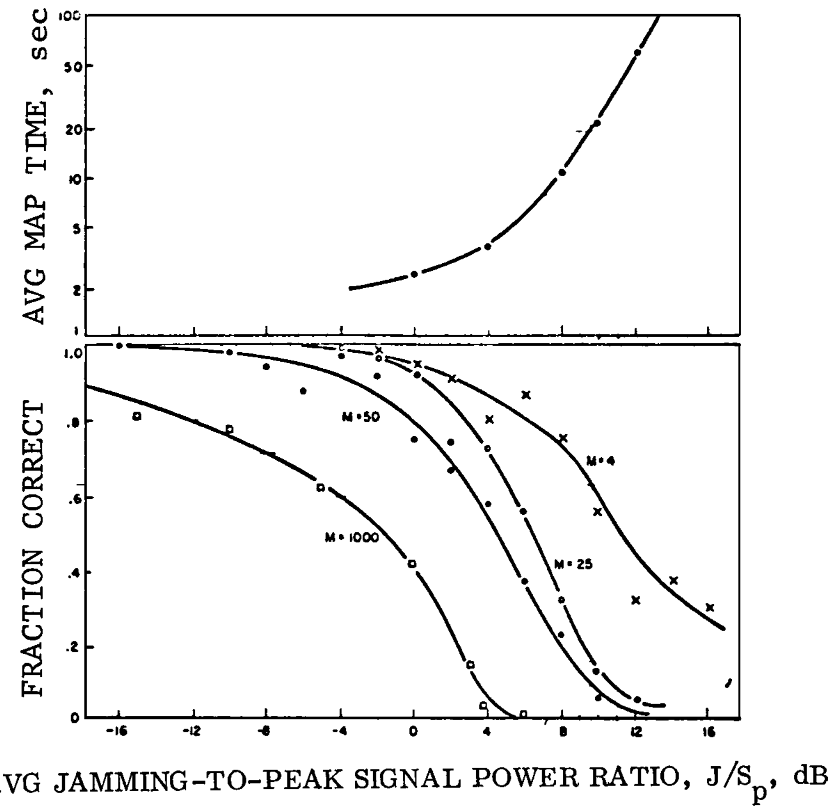
3-2.1.2.3 (U) Map Test (Refs. 14, 15)

The Map Test is one approach to the problem of attempting to remove some of the objections to the articulation testing procedure, these being the lack of consideration for the time of message transmission, the failure to allow structure or redundancy in the transmitted message, and the lack of opportunity for feedback to be incorporated. All of these characteristics appear in military transmissions. A consequence of these considerations was the development of the "Map Test" (also called the Michigan Map Test) by the Electronic Defense Group at the University of Michigan (Refs. 16, 17). The basic idea is represented in Figs. 3-6 and 3-7. The transmitting observer selects one of a limited ensemble of 972 possible routes on a grid of "towns" whose names are the letters of the phonetic alphabet. Each route of six towns represents a fixed amount of information, 9.925 bits, to be transmitted in a minimum and measured amount of time when jamming is being employed. The receiving operator records the route received on a similar grid. Various forms of feedback may be employed such as a noise-free channel, a jammed channel, or a low-capacity channel with a light to signal the transmitting operator to proceed with the transmission.

The limited choice available to the transmitter at each intersection is representative of the structured redundancy of the map; the receiving operator knows that only a limited choice is possible. The measured time for transmission (called the "map time") can be taken as the jamming effectiveness for each J/S and for each experimental arrangement of parameters. By way

of reference, a six-town map can be transmitted in the clear in about 2 sec by trained observers; if they require more than 20 sec for transmission under jamming conditions, they stand a very small chance of getting the message through at all.

The Map Test gives excellent quantitative results in the laboratory. However, it is not possible or even feasible to interpret the results of this test in terms of practical field conditions or even other methods of testing such as an intelligibility test. However, as a possible aid to interpreting results obtained from map tests, comparisons—although subject to many flaws—of results from both a map test and an articulation test under the same jamming conditions have been made. Results are shown in Fig. 3-8. The test was performed strictly at baseband in a linear, audio channel with the presence of added white Gaussian noise. In Fig. 3-8 the upper portion represents map time as a function of J/S_p (average jamming power to peak enve-



$B_a = B_n$ = 250 to 3500 Hz

NORMAL SPEECH M= VOCAB SIZE

SLOW ALC (R ≈ 10 dB/sec)

Figure 3-8 (U). Comparison of Map Test and Intelligibility Score Test for an Audio Channel With Additive Gaussian Noise (U)

lope signal power); the bottom portion represents the fraction of correct responses in the articulation test as a function of J/S_p for different vocabulary sizes. From Fig. 3-8 it is seen that a map time of 20 sec corresponds to a J/S_p of nearly 10 dB, which corresponds to articulation scores, as a function of vocabulary size, shown in Table 3-2.

3-2.1.2.4 (U) Character Error Rate

In a communication system such as one that transmits radio teletype it is more meaningful for a user to specify or measure performance in terms of the number of teletype characters that are in error rather than in terms of bit error rate. For example, an error rate might be specified as one character error in five lines of copy. For start-stop teletype (one start pulse, one stop pulse, and five information pulses per character) containing 66 characters per line, this corresponds to a bit error rate of 4×10^{-4}. Clearly, the statement of one character error in five lines is more meaningful to a user than the statement that the ber is 4×10^{-4}.

This method of expressing an error rate has the disadvantage that higher error rates are difficult to count from teletype copy. Because of this difficulty the jammed condition of radioteletype usually is expressed as the point at which sync is lost rather than as character error rate. (See par. 3-2.1.4.)

3-2.1.2.5 (U) Relative Message Delay

The Relative Message Delay criterion is similar to the Map Test, but it can apply to many different kinds of messages; e.g., voice or manual morse, long or short. It is simply the ratio of time required to transmit the same message successfully with jamming and without jamming. As with the Michigan Map Test, a tenfold increase in time required to transmit a message often is taken as the jammed condition.

3-2.1.2.6 (U) Signal-to-Noise Ratio and Related Measures

The output of a receiver can be characterized by its signal-to-noise ratio S/N. However, depending on the character of the signal, it may be difficult to separate signal and noise so each one can be measured separately to obtain the S/N. Nevertheless, it is possible for a listener to evaluate subjectively, on a voice transmission for example, whether the S/N is high or low. High S/N correlates with high intelligibility and low S/N with low intelligibility.

One method of measuring S/N is to insert, as the signal, a test tone such as 1000 Hz. It is inserted at a fixed power level and a known modulation index. At the receiver output the power of the test tone can be measured after first filtering it out with a

TABLE 3-2 (U). ARTICULATION SCORE IN A BANDLIMITED AUDIO CHANNEL WITH ADDITIVE WHITE GAUSSIAN NOISE FOR THE SAME J/S_p (≈10 dB) THAT RESULTS IN A MAP TIME OF 20 SEC (U)

Vocabulary Size, M	Articulation Score, %
4	65
25	15
50	8

very narrow filter. The noise is measured across the entire output bandwidth except for the narrow slot containing the test tone. This S/N is sometimes called "test tone-to-noise ratio" TT/N. When a tone is used as the signal to test an fm receiver, a comparison is usually made between the carrier-to-noise C/N ratio at the receiver input and the S/N at the receiver output. Par. 3-2.2.1.1 shows a plot of such a comparison.

Another method measures the ratio of signal plus noise-to-noise, expressed by the term $(S + N)/N$. This is an easier measurement. The average output power of the receiver is measured first with the signal present and then with signal modulation turned off. A common standard for satisfactory communications often used is $(S + N)/N \geqslant 15$ dB (sometimes 13 dB).

The previous method suggests another that is not often used for EW vulnerability evaluation, although it is common in telephony work. This is simply to measure the noise power that is present in a voice channel without a signal present on that channel. A discussion of the method can be found in standard references on the measurement of noise in communication circuits.

3-2.1.3 (U) Jamming-to-Signal Ratios *(J/S)*

3-2.1.3.1 (U) Measures of *J/S*

When susceptibility is plotted as receiver performance vs J/S, the signal and jamming powers in the J/S may be average power, peak envelope power, or carrier power. Which particular power measure is appropriate depends on the modulation, the particular modulation waveform, and the equipment power-handling capability (Ref. 17). Of course, the power measure that is used for the J and S terms of the J/S must be specified so that the susceptibility curve has meaning. It is not necessary that both J and S be the same measure. For example, J could represent carrier power and S could represent peak envelope power.

A common but not universal convention often used to discuss the susceptibility of single-channel voice communications is to specify J as the average power in the jamming signal and S as the peak envelope power of the target signal. The ratio is written as J/S_p as a reminder that S is a measure of peak envelope power, not average power. The use of a peak envelope power measure for the target signal is employed because it is the most general, applicable to am, fm, and ssb alike. It is appropriate, too, because frequently transmitters are peak-power-limited. For full carrier am the peak envelope power S_p is 6 dB greater than the carrier power S_c; for fm the peak envelope power, the average power, and the carrier power are all the same; for ssb the peak envelope power S_p is the most meaningful measure because the average power can fluctuate considerably with the modulating voice waveform and may be of the order of 6 to 12 dB lower in power than the peak envelope power.

3-2.1.3.2 (U) Variation of Required *J/S* With Signal and Equipment Parameters

The susceptibility threshold—i.e., the J/S required to jam—usually varies as a function of any parameter that can be changed, whether it is a parameter of the jamming signal, of the target signal, or of the target receiver. Fig. 3-9 demonstrates this for a single parameter change first in the receiver, then in the target signal, and then in the jamming signal. These curves were generated in a susceptibility test program against manual morse transmissions (Ref. 18). The jamming signal for the curves of Fig. 3-9 was random manual morse at approximately the rate of the target signal, turning a carrier off

and on; at the same time the carrier was being frequency-modulated by a sawtooth at various deviations. In the absence of jamming, a message could be transmitted in about 25 sec. A tenfold increase in average message time was selected as the jammed condition, i.e., an average message time of 250 sec. In Fig. 3-9(A), the wider bandwidth of the receiver apparently let more jamming power into the receiver, so that jamming was easier. In Fig. 3-9(B), offsetting the signal from the jamming in frequency appears to avoid a large portion of the jamming power so that the signal was not jammed. In Fig. 3-9(C) an increase in the frequency deviation placed some of the jamming power outside the receiver bandpass; the remaining jamming power was "spread thinner", and so jamming was less effective.

Similar results are observed for nearly all combinations of receiver, signal, and jamming.

3-2.1.3.3 (U) Processing Gain

The J/S required to jam a signal is affected by a characteristic of the target signal and receiver in combination that is called the processing gain. Processing gain can be thought of either as the ratio

$$\text{Processing Gain} = \frac{\text{Rf bandwidth of the receiver}}{\text{Information bandwidth of the signal}}$$

or

$$\text{Processing Gain} = TB \tag{3-1}$$

where

T = bit duration, sec = $\dfrac{1}{\text{data rate}}$

B = receiver rf bandwidth, Hz

These two definitions are equivalent; the first is more easily applied to analog modulation and the second to pulse modulation.

The relation between the J/S required to jam and processing gain is

$$\left(\frac{J}{S}\right)_{dB} = (\text{Processing Gain})_{dB} - \left(\frac{E}{N_0}\bigg|_{\text{critical}}\right)_{dB} \tag{3-2}$$

where

E/N_0 critical = E/N_0 required to give the error rate chosen to be the jammed condition (see par. 3-2.2).

E = energy in one bit, J

N_0 = noise power density, J or W · Hz^{-1}

Processing gain and its effect on the J/S required to jam can be visualized by an example of rf noise jamming against binary fsk. First, approaching the problem heuristically, suppose a target signal transmits 100-bit-per-sec data by noncoherent fsk, modulating a carrier ± 100 Hz. Jamming is then carried out by placing bandlimited Gaussian noise over the target signal so that it just covers the useful spectrum of the target signal; power in the jamming signal is the minimum amount required to jam—i.e., to produce the error rate that has been selected as the jammed condition. Now, if the data rate remains constant but the carrier is modulated ± 500 Hz, the rf bandwidth B of the receiver must be increased to match the transmitted bandwidth. It is apparent that, in order to continue jamming, the bandwidth of the noise must be increased and, in order to keep the noise at the same power level across this bandwidth, the total noise power of the jamming signal must be increased; i.e.,

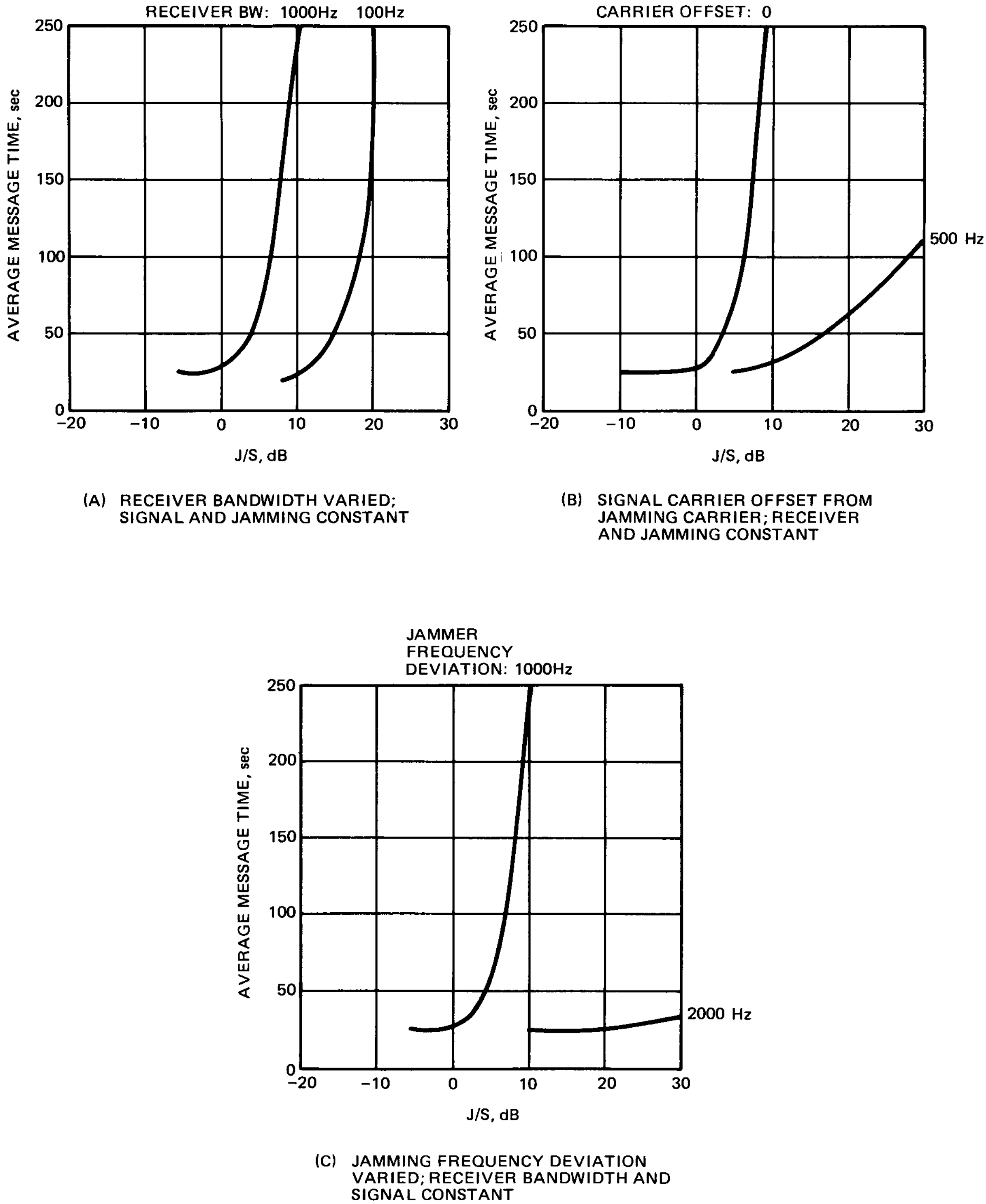


Figure 3-9 (U). Effect of Variations of Signal, Jamming, and Receiver Parameters on J/S *(U)*

an increase in processing gain by increasing B requires an increase in J (jamming power) to maintain the same level of jamming. In either case, maintaining a constant signal power but increasing the processing gain requires an increase in the J/S in order to maintain the same level of jamming.

Approach the same problem quantitatively. Assume the jammed condition is selected to be $P_e = 10^{-3}$; the value of E/N_0 that causes this probability of bit error P_e can be obtained from (see par. 3-2.2):

$$P_e = (1/2) \exp\left(-\frac{E}{2N_0}\right) \tag{3-3}$$

Solving, $10^{-3} = (1/2) \exp [-E/(2N_0)]$ gives $E/N_0 = 12.43 = 10.93$ dB or $E/N_0 \cong 11$ dB. That is, jamming to produce a bit error rate of 10^{-3} must be present with sufficient noise power density so that the ratio of energy in one bit to noise power density is 11 dB. To overcome the processing gain, additional jamming power is needed. Suppose B is twice the peak-to-peak carrier swing. Then

B = 400 Hz for ± 100-Hz fsk

B = 2 kHz for ± 500-Hz fsk

For the two data rates of this example

T = 10 msec for 100 bps

T = 13.3 msec for 75 bps

When B = 400 Hz and T = 10 msec, processing gain is, by Eq. 3-1,

TB = 4 (6 dB)

When B = 2 kHz and T = 10 msec, processing gain is

TB = 20 (13 dB)

When B = 400 Hz and T = 13.3 msec, processing gain is

TB = 5.3 (7.3 dB)

Calculating the relationship J/S required to jam for each of these conditions, using $J/S = TB - E/N_0$, gives

J/S = 6 - 11 = -5 dB for T = 10 msec, B = 400 Hz

J/S = 13 - 11 = + 2 dB for T = 10 msec, B = 2 kHz

J/S = 7.3 - 11 = -3.7 dB for T = 13.3 msec, B = 400 Hz

Note that if receiver bandwidth B had just been matched to the bit duration by $B = 1/T$, then processing gain TB = 1 (0 dB) and noise jamming would have occurred at J/S = −11 dB. However, in all three instances in this example, a higher J/S was required because of the presence of a processing gain that was greater than unity (0 dB).

3-2.1.3.4 (U) Environmental Noise and Interference

For a communication system in actual use, there is always some interfering noise present at the receiver input even in the absence of jamming. This can be naturally occurring noise, unintentional interference from man-made noise, interfering communication systems, or some combination of these. Thus, the input S/N, at the receiver is always noninfinite. This noise degrades receiver performance the same as jamming does. In a jamming environment the already-present noise may contribute to the jamming power. In recognition of this the J/S is sometimes replaced with the ratio $(J + N)/S$ [or its reciprocal $S/(J + N)$ may be used].

In general the effects of interference and environmental noise are more serious for digital communication systems than for analog systems. The presence of noise and interference in the field makes jamming easier than laboratory susceptibility tests under ideal conditions might indicate, but this is, as a general rule, more pronounced for digital systems.

3-2.1.4 (U) Susceptibility Thresholds

3-2.1.4.1 (U) Discussion of Thresholds

Susceptibility to jamming (for a fixed set of parameter values on a target signal, jamming signal, and target receiver) can be described by a curve of performance vs *J/S*. Various ways of describing performance are discussed in par. 3-2.1.3; several measures for describing *J/S* are discussed in par. 3-2.1.3. The jammed condition is any performance less than some threshold performance on the ordinate of the susceptibility curve. Selection of this performance threshold is covered in par. 3-2.1.4.2. The *J/S* on the abscissa of the susceptibility curve that produces this performance threshold is called the susceptibility threshold.

3-2.1.4.2 (U) Selection of Performance Thresholds

The performance that the analyst selects as the threshold between the jammed and the unjammed condition should be one that is appropriate both to the operational use of the communication system and to the modulation the system uses.

(1) *Analog Voice.* The performance selected as the threshold between the jammed and nonjammed condition for analog voice systems—e.g., tactical, single channel am, fm, or ssb—usually is stated in terms of intelligibility or message delay. The purpose of analog voice communication systems is to transmit the human voice intelligibly; thus intelligibility is a more logical and direct measure of performance than a quantity such as output signal-to-noise ratio would be. However, the percent intelligibility that is acceptable to the user is still a subjective kind of decision. Moreover, if he must decide on what percentage of intelligibility of a phonetically balanced word list he will accept, this percentage first must have some meaning to him in terms of what equivalent degradation he will experience in his normal voice communications. The redundancy of the language and the relatively small size of the vocabulary used on a tactical network will result in a higher percentage of words received correctly than the PB word list score indicates. Moreover, the tactical net permits the user to ask for repeats of words he did not receive intelligibly. So, while the user needs intelligibility from his voice network, he often considers the time required to get his message through intelligibly as a better indication of the grade of service. Therefore, a measure such as Map Time or Relative Message Delay very often is used to describe performance.

Tests using the Michigan Map Time as a measure of performance have found that, if the message cannot be transmitted in 20 sec (average time without jamming is 2 sec), there is a high probability of never getting it through. Therefore, 20 sec often is taken as the performance threshold and the *J/S* that corresponds to 20 sec of map time is taken as the susceptibility threshold. Similarly, tests that use messages of other lengths often take the equivalent—a tenfold delay in transmission time over that required in the absence of jamming—as the performance threshold.

(2) *Digital Voice.* In some communication systems voice is digitized and then encoded by some pulse modulation technique, pcm for example. This is done commonly on time-division multiplex, multichannel

trunk communications. In addition to encoding the digitized voice by pulse code modulation (pcm), the pcm bitstream itself often is encrypted before transmission, then decrypted on the receiving end. Jamming and other interference usually affect voice transmissions that have been digitized in a different way than that by which they affect analog voice transmissions. Analog voice transmissions usually degrade gracefully in quality with an increase in jamming power; digitized voice transmissions usually degrade very little up to a threshold and then fail catastrophically as the jamming is increased further. Generally this failure occurs as the result of loss of synchronization between the incoming bitstream and the timing in the receiver. As this failure threshold is crossed, the intelligibility changes rapidly from a value that is so high it is difficult to count, down to essentially zero. However, the change in ber in the bitstream is not nearly so rapid. The ber at which loss of synchronization occurs can be identified readily. Therefore, it is common to specify the performance threshold of these systems in terms of ber and the susceptibility threshold as the J/S that produces that ber. In some typical tests (Ref. 19), synchronization was lost for $10^{-1} < \text{ber} < 3 \times 10^{-1}$.

(3) *Radioteletype.* The most reliable and practical performance threshold for radioteletype is "total loss of teletype synchronization". Even though this is not a quantitative threshold, it is fairly easy to detect. Moreover, it represents a truly jammed condition because, when sync has been lost, the intended recipient receives no information from the sender. Tests (Ref. 20) have shown that, for several jamming signals, intermittent loss of teletype sync occurs at a J/S of about 2 or 3 dB higher than the J/S that causes one character error in five lines.

Examples of typical tty printouts obtained during a test program (Ref. 20) are shown in Fig. 3-10. Fig. 3-10(A) is representative of one character error in five lines (the 13th character in line 2). At a J/S typically 2 or 3 dB higher, the copy shown in Fig. 3-10(B) is obtained. Note that the 6464 · · · sequences are actually RYRY · · · preceded by a character error mistaken for a carriage shift to numerals. Also, there is a large number of line feeds and carriage returns. Finally, the copy in Fig. 3-10(C) represents a total loss of teletype synchronization as indicated by the absence of either RYRY · · · or 6464 · · · . This copy is obtained at J/S's 4 to 5 dB above those that produce copy like that of Fig. 3-10(A).

If a character error rate is selected as the performance threshold that is less than the out-of-sync condition, Fig. 3-11 may be used to translate that character error rate to bit error rate.

(4) *Other Data.* In addition to digital voice and radioteletype, there are many other kinds of digital transmissions. For example, digital data can be transferred between computers or other processors; data can be transmitted from remote sensors to a central processor; and radar displays can be encoded digitally and transmitted for remote viewing. Each kind of transmission will have its own performance threshold beyond which the users consider it too degraded to use. In many cases this threshold is a ber less than the ber at which loss of system sync occurs. In other cases systems can operate right up to the loss of sync threshold. If the ber is critical for a system—for example if a system cannot tolerate more than one error in 10^{-5} bit—hardware may be added to detect and correct errors (error detection and correction equipment). This equipment adds bits to the bitstream. If the ber of the full bitstream (information bits and error correction bits) is measured, it may measure 10^{-4}, but the errors that occur in the information bits are being corrected so that, upon removal of the error correction bits,

```
RYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRY
RYRYRYRYRYRYHTRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRY
RYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRY
RYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRY
RYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRYRY
```

(A) ONE ERROR IN FIVE LINES OF COPY

```
4646464144464644&65646'646464646464&64646464646414646444146464646
-4646464646463
                ..-,4&664
                  ..      64644
663-3,)2,                        646(64/:646$326!'646
         )464649                          ..   ..
                     64646:646643(6'64646464446464/4/414646
                                                                6  33-6(6946'646
6&66868664£5466!65464646
```

(B) PARTIAL LOSS OF TTY SYNCHRONIZATION

```
   !:NFVUKWBB AZR? 5.$.4!'";:1"                         ..
}8814(59 $7                           4!H'"'5 ",?&4
RVPPAX 9;08-'?:787(5VOCMMRGHFLFYDZO                   ..
VXBDMCLKVSHLM VCQARQGYCXHH

; ') 56&
;7:C 0!!18&1&'!)1".-(
,7 KTAQJOGHUHWPFRRYXV8'
  "//:2 88                 ..
```

(C) TOTAL LOSS OF TTY SYNCHRONIZATION

Figure 3-10 (U). Typical Teletypewriter Printouts (U)

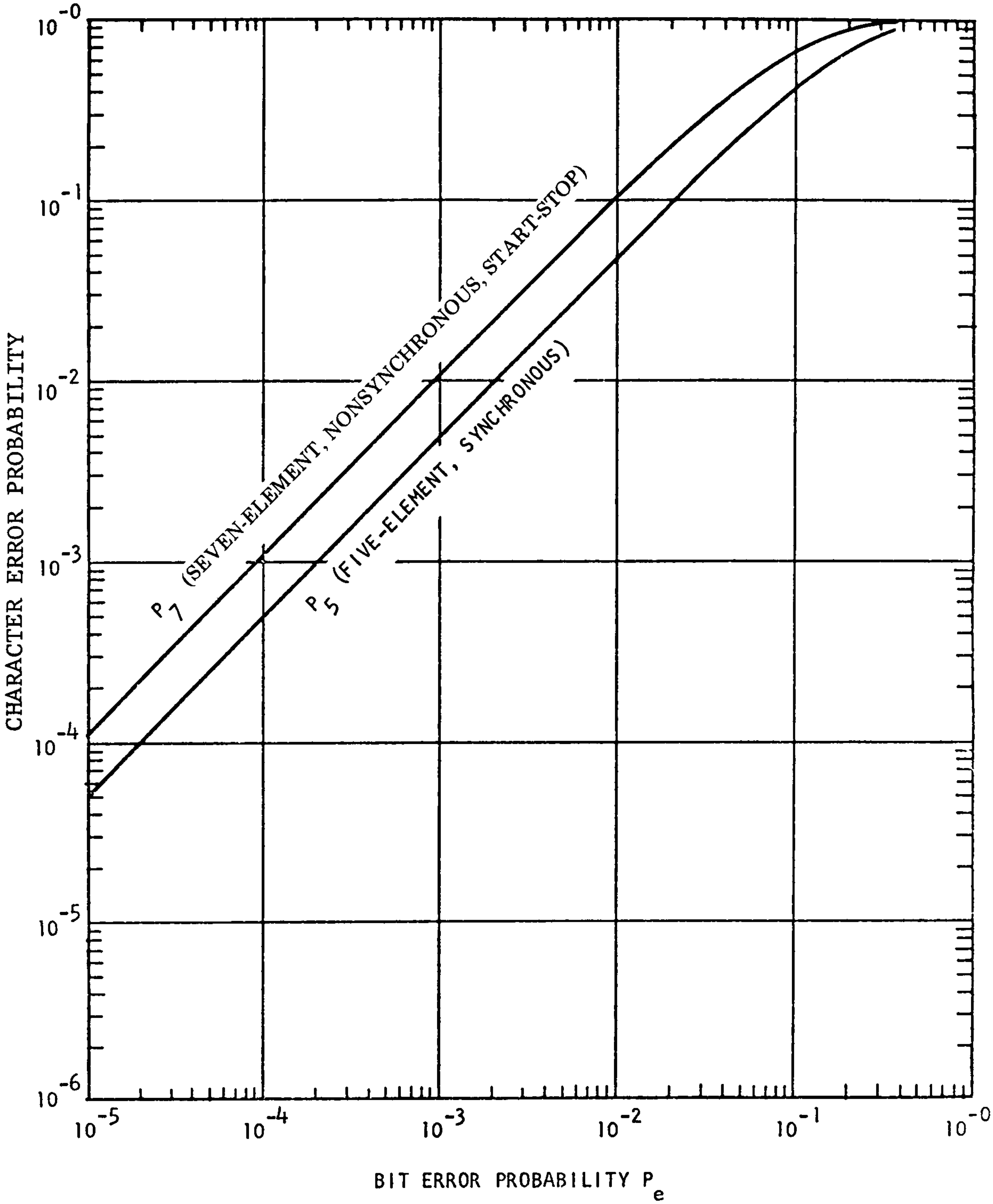


Figure 3-11 (U). Character Error Probability as a Function of Bit Error Probability for Two Teletype Codes (U)

INDEX

Index Terms	**Links**	

F

Index Terms	**Links**

G

J

K

L

Index Terms	Links	

O

P

Index Terms	Links	

Index Terms	**Links**	